Східноєвропейський національний університет імені Лесі Українки
Факультет економіки та управління
Кафедра економіки, безпеки та інноваційної діяльності підприємства

Анна Мохнюк
Олена Скорук

ОРГАНІЗАЦІЯ ТА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ПІДПРИЄМСТВІ

Конспект лекцій

Луцьк
2017

УДК [334:338.2]:001.92(075)
ББК 65.291.573я73-2
М 44

Рекомендовано до друку науково-методичною радою Східноєвропейського національного університету імені Лесі Українки (протокол № 6 від 15.03.2017 р.)

Рецензенти:

Ліпич Л. Г., д.е.н., професор, декан факультету економіки та управління Східноєвропейського національного університету імені Лесі Українки

Савош Л. В., к.е.н., доцент, зав. кафедри економічної теорії та міжнародної економіки Луцького національного технічного університету

Мохнюк А. М., Скорук О. В.
М-44 Організація та управління інформаційною безпекою на підприємстві: конспект лекцій / Укладачі Анна Миколаївна Мохнюк, Олена Володимирівна Скорук. – Луцьк : ПП «Поліграфія», 2017. – 99 с.

У навчальному виданні узагальнено теоретичні та методичні засади інформаційної безпеки в підприємницькій діяльності, визначено основні загрози інформаційній безпеці та особливості управління системою інформаційної безпеки на підприємстві.

Рекомендовано студентам 6 курсу спеціальності 073 «Менеджмент» освітньої програми «Управління фінансово-економічною безпекою».

УДК [334:338.2]:001.92(075)
ББК 65.291.573я73-2

ЗМІСТ

Передмова

Метою викладання навчальної дисципліни «Організація та управління інформаційною безпекою на підприємстві» є формування системи спеціальних знань з питань організації та управління інформаційною безпекою на підприємстві.

Основними завданнями вивчення дисципліни «Організація та управління інформаційною безпекою на підприємстві» є вивчення основних теоретичних положень дисципліни; з'ясування сутності та основних положень інформаційної безпеки в підприємницькій діяльності; визначення основних загроз інформаційній безпеці підприємства; формування знань, умінь та творчого підходу при розробці та управлінні системою інформаційної безпеки на підприємстві.

Після опанування дисципліни студент повинен:

знати:

категорії та основні поняття в сфері інформаційної безпеки підприємства; особливості організації інформаційної безпеки на підприємстві; правові засади інформаційної безпеки підприємства; основи побудови і функціональні можливості інформаційних систем; правила, методи і засоби підготовки технічної документації; методи оцінки ефективності впровадження інформаційних систем; призначення, склад і принципи функціонування інформаційних ресурсів організації; національні, галузеві стандарти і стандарти підприємства відносно інформаційних систем; методи аналізу надійності і якості інформаційних систем, сертифікації і атестації інформаційних систем і їх компонентів, державні і міжнародні стандарти;

вміти:

– оцінювати стан інформаційної безпеки на підприємстві;

– організовувати захист інформації з обмеженим доступом на підприємстві;

– характеризувати загрози інформаційній безпеці підприємства, розробляти заходи щодо їх уникнення та нейтралізації;

– розробляти пропозиції щодо удосконалення управління інформаційною безпекою на підприємстві;

– розробляти методи і схеми тестування й випробування інформаційнихсистем;

– визначати склад і функціональні характеристики інформаційних систем;

– документувати і аналізувати проблеми, пов'язані з функціонуванням систем і варіанти їх рішення;

– організовувати і координувати роботу щодо експлуатації і супроводу інформаційних систем; тощо.

Структура навчальної дисципліни

Назва змістових модулів і тем	Кількість годин				
	Усього	у тому числі			
		Лек.	Практ. (Семін.)	Конс.	Сам роб.
1	2	3	4	5	6
Змістовий модуль 1 Теоретичні основи організації інформаційної безпеки на підприємстві					
Тема 1. Інформація та інформаційні системи	10	2	2	1	5
Тема 2. Поняття інформаційної безпеки на підприємстві	10	2	2		6
Тема 3. Основи організації інформаційної безпеки на підприємстві	10	2	2	1	5
Тема 4. Особливості захисту інформації на підприємстві	11	2	2	1	6
Разом за змістовим модулем 1	41	8	8	3	22
Змістовий модуль 2 Інформаційне забезпечення діяльності підприємства та управління інформаційними ризиками					
Тема 5. Правові засади інформаційної безпеки підприємства	8	1	1		6
Тема 6. Інформаційне забезпечення діяльності підприємства	9	1	1	1	6
Тема 7. Політика інформаційної безпеки підприємства	11	2	2	1	6
Тема 8. Управління інформаційними ризиками на підприємстві	11	2	2	1	6
Тема 9. Концепція технічного захисту інформації на підприємстві	10	2	2		6
Разом за змістовим модулем 2	49	8	8	3	30
Усього годин	90	16	16	6	52

ЗМІСТОВИЙ МОДУЛЬ І
ТЕОРЕТИЧНІ ОСНОВИ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

ТЕМА 1
ІНФОРМАЦІЯ ТА ІНФОРМАЦІЙНІ СИСТЕМИ

1.1. Інформаційний розвиток та його особливості
1.2. Сутність інформаційного середовища та його інфраструктура
1.3. Основні характеристики та класифікація інформації
1.4. Поняття інформації з обмеженим доступом
1.5. Інформаційні системи: сутність та класифікація

1.1. Інформаційний розвиток та його особливості

Сьогодні домінуюча роль інформації у розвитку суспільства є очевидною. Інформаційний розвиток, пов'язаний із розвитком знань та інтелектуалізацією суспільства, обумовлює нові підходи у взаємовідносинах різних суб'єктів від громадян і до міжнародних відносин.

Водночас необхідно звернути увагу на особливості інформаційної складової саме в сьогоднішніх умовах. Справа у тому, що інформаційна складова була завжди присутня в діяльності людства, будь-який вид громадського, економічного, технічного розвитку в тій чи іншій мірі був пов'язаний із інформаційним забезпеченням. Досягнення практично у всіх сферах життєдіяльності базувались на інтелектуальних здобутках, які перш за все характеризувались інформаційно.

Домінуюча роль інформації в розвитку суспільства пояснюється такими факторами:

– значним чином збільшились обсяги інформації. Будь-яка діяльність, сфера, взаємовідносини характеризуються не просто великими обсягами інформації, а такими, що у звичайному режимі її сприйняття опанувати неможливо. Так, за останні 35 років у світі вироблено більше інформації, ніж за 5 тис. років до цього. Підраховано, що один примірник газети «Нью-Йорк Таймс» містить інформації більше, ніж її міг отримати мешканець Англії за все життя.

Подвоєння знань з 1900 р. здійснювалось кожні 50 років, з 1950 р. подвоєння проходило вже кожні 10 років, з 1970 р. – кожні 5 років, а з 1990 р. – щорічно. Якщо обсяги інформації будуть зростати такими темпами, то кількість знань для людини збільшиться в мільйони разів, виникне суттєвий розрив між обсягами інформації і спроможністю не тільки її засвоїти, а навіть зрозуміти. Більш того, інформаційні характеристики існують як об'єктивно, так і природньо чи штучно викривленими, що значно доповнює обсяги інформації та вимагає обов'язкової її обробки;

– в останні роки збільшились темпи зміни інформаційних характеристик. На відміну від минулих років повне оновлення інформації здійснюється один раз в 7 років. Така ситуація обумовлює необхідність швидкого впровадження в

практику суспільної діяльності та використання інтелектуальних досягнень. В свою чергу, швидкий обіг інформації вимагає постійного пошуку необхідних відомостей, що робить інформаційну роботу завжди актуальною та такою, що є невід'ємною складовою будь-якої діяльності в сучасних умовах;

– наявність великих обсягів не завжди об'єктивної інформації, швидка зміна інформаційних характеристик, а також можливість отримати певні переваги за рахунок інформації у суспільних взаємовідносинах зумовило необхідність формування суб'єктами зазначених відносин власного інформаційного ресурсу. Тобто, в даний час суспільний розвиток не може забезпечуватись лише фінансовими, матеріальними, кадровими ресурсами, а вимагає ще і відповідних інформаційних ресурсів;

– інформація на сьогодні існує не тільки як певна сума знань, а і як відповідний технологічний процес, який у поєднанні з іншими технологіями може суттєво впливати як на розвиток суспільства в цілому, так і на окремі його елементи. Зазначені технології здатні прискорювати або навпаки сповільнювати темпи суспільного розвитку, забезпечувати переваги розвитку окремих сфер, галузей чи концентрувати суспільні зусилля на певних напрямах. Більш того, інформаційні технології здатні формувати характер взаємовідносин у суспільстві, від мирного співіснування до суттєвих конфліктів. Здатність інформаційних технологій впливати на характер взаємовідносин у суспільстві обумовила сьогодні появу нового виду зброї – інформаційної, застосування якої несе в собі не менш негативні насліди, ніж від зброї в звичайному розумінні цього слова;

– сучасний рівень розвитку демократизації та технічного прогресу зумовив значне розширення доступу до інформації. Насамперед, збільшилось коло осіб здатних отримати необхідну їм інформацію, знизився рівень закритості інформації, значно збільшилась кількість джерел інформації. Глобалізація суспільних та економічних відносин дає можливість отримувати інформацію практично з будь-якого сегменту інформаційного простору.

Однією з важливих особливостей сучасного інформаційного розвитку є те, що значне збільшення обсягів інформації та розширення можливостей її використання забезпечило становлення нового етапу суспільного розвитку, однією з характеристик якого є суттєве зростання інтелектуального потенціалу в структурі всіх його процесів.

Зміни, що відбулись в останні роки в інформаційному середовищі суспільства призвели до нового ставлення до інформації. Остання стала необхідною складовою життєдіяльності, що сприяло формуванню т. з. інформаційного мислення, а з ним і нового виду відносин – інформаційних. Тобто, можна говорити, що зміни в інформаційному просторі призвели до формування інформаційного образу життя людини та інформатизації суспільства. Інформація стала зачіпати всі сторони суспільного життя. У суспільства, громадян, організацій, господарюючих суб'єктів з'явилась постійна потреба у інформації, її продуктах. У зв'язку з такою потребою з'явились відповідні види діяльності, в основі яких є інформація, як то вироблення інформаційної продукції, забезпечення передачі інформації,

формування інформаційних ресурсів, захист інформації, поширення інформації, надання різного роду інформаційних послуг (збір інформації, її обробка, розробка інформаційних комп'ютерних програм, технологій та ін.).

Таке активне зростання ролі інформації значним чином підвищило її цінність у взаємовідносинах та виробництві, а з цим і ціну її продуктів. Тобто, інформація, її продукти стали товаром, що зумовило появу інформаційного ринку та інформаційної індустрії, а властивість інформації впливати на індивідуальну чи колективну свідомість, утворила можливість здійснення т. з. інформаційних війн.

Під впливом масштабного розвитку інформації відбулися зміни трудової діяльності людини, господарської та інших видів діяльності юридичних суб'єктів, суспільних відносин. Серед основних характеристик таких змін можна назвати:

– відбулось скорочення часу у циклах управління та виробництва за рахунок інформатизації та автоматизації їх процесів;

– засобами виробництва стала комп'ютерна техніка, яка дозволила спростити процес вироблення продукції, а комп'ютерні технології зумовили мінімізацію участі людини в ньому і тим самим зменшили собівартість продукції;

– стала можливою технологічна і географічна інтеграція у всіх сферах життєдіяльності: економічній, суспільній, освітній, військовій та ін., наукові здобутки можуть швидко перетворюватись у реальні технології, засоби, поведінку, а можливості регіонів чи навіть країн оптимально поєднуватись для вирішення актуальних завдань життєдіяльності;

– підвищилась надійність технологій, заснованих на штучному інтелекті і запроваджених в управлінні та виробництві;

– відбулось становлення та розвиток єдиного інформаційного простору як певної сукупності інформаційних ресурсів та інформаційних технологій, які дозволяють використовувати їх у різних видах діяльності різними суб'єктами на основі регульованого доступу;

– розширився світогляд громадян та відбулось удосконалення їх інформаційної культури, з'явилась можливість застосування отриманих з інформаційних мереж знань для забезпечення їх життєдіяльності;

– відбувся перерозподіл видів трудової діяльності, значна її частина перебуває зараз в інтелектуальній сфері, що підвищує інтелектуальний потенціал суспільства і вимагає уточнення напрямів його подальшого розвитку;

– інформаційні зміни створили передумови для суттєвих перетворень в економіці, де вирішальну роль в економічній діяльності буде відігравати інформація і її технології.

Таким чином, можна говорити не лише про появу нового виду діяльності – інформаційної, а і про те, що вона є досить динамічною та з великим потенціалом розвитку, а і про те, що така діяльність має значні перспективи. Тобто, рівень інформаційного розвитку стає важливою характеристикою не лише сучасного суспільства, а і провідними показником конкурентоздатності

суб’єктів підприємництва, якраз через нього може визначатись їх потужність на ринку.

Інформатизація суспільства активізувала проведення наукових досліджень у різних сферах його життєдіяльності, результати яких склали основу подальшого розвитку як окремих його суб’єктів, так всього суспільства. Наприклад, інформаційний вибух у засобах комунікацій, який відбувся у останні 15-20 років зумовив потребу у нових наукових розробках засобів зв’язку, насамперед мобільного.

Інформаційний розвиток не лише зумовив значне зростання обсягів інформації, швидкості її зміни та прибрав кордони її поширення, а і суттєво поновив інструменти застосування інформації, насамперед інформаційні технології. Характерною рисою сьогоднішніх інформаційних технологій є проникнення їх практично до всіх сторін життєдіяльності суспільства. Інформаційні технології стали застосовуватись у взаємозв’язку з технологіями та методиками інших сфер: економічної, соціально-психологічної, правової та ін. Від цього вплив інформаційного розвитку стає ще більш значним для суспільства та взаємовідносин суб’єктів.

1.2. Сутність інформаційного середовища та його інфраструктура

Інформаційне середовище існує у сукупності певних елементів, які формують його інфраструктуру. Разом з тим, інформаційна інфраструктура має свої особливості, обумовлені специфікою функціонування та призначення інформації.

Інформаційне середовище – це сукупність суб’єктів, засобів (технологій), ресурсів та зв’язків, які забезпечують створення, передачу та споживання інформації і дії, що супроводжують та забезпечують ці процеси.

В той же час, незважаючи на існування визначення даного поняття в правових документах держави, серед фахівців та науковців точиться певна полеміка щодо найбільш оптимального та грамотного його розуміння.

Найбільш цілісним та змістовним є визначення інформаційної інфраструктури, подане в Стратегії розвитку інформаційного суспільства в Україні. Зокрема, під **інформаційною інфраструктурою** пропонується вважати сукупність різноманітних інформаційних (автоматизованих) систем, інформаційних ресурсів, телекомунікаційних мереж і каналів передачі даних, засобів комунікації і управління інформаційними потоками, а також організаційно-технічних структур, механізмів, що забезпечують їх функціонування.

Елементи інформаційної інфраструктури:

– інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

– телекомунікаційна мережа – це комплекс технічних засобів телекомунікації та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень

та звуків або повідомлень будь-якого роду по радіо, проводних, оптичних чи інших електромагнітних системах між кінцевим обладнанням;

– канал передачі даних – комплекс технічних і програмних засобів, що забезпечують передачу цифрової інформації різними середовищами;

– засоби комунікації – засоби, що застосовуються для передачі, оголошення, обміну інформації в усному, письмовому чи візуальному видах поміж різними суб'єктами, можна робити висновок про наповнення інформаційної інфраструктури переважно електронними засобами роботи з інформацією;

– інформаційні ресурси – інформація вільного доступу (продукція засобів масової інформації, правові документи, реєстри, наукові роботи та видання, матеріали соціологічних та інших досліджень, повідомлення органів статистики, державних органів та установ, архівні документи, навчальна література, матеріали мережі Інтернет, продукція інформаційного ринку, аналітичні документи (огляди, прогнози), енциклопедичні та довідникові матеріали, рекламні продукти, агітаційні та пропагандиські матеріали, виставкові експозиції, індивідуальні та колективні знання, матеріали технологічного характеру);

– суб'єкти – юридичні і фізичні особи, що відповідно до законодавства здійснюють легальну діяльність у сфері вироблення, збереження, поширення та використання інформації.

Особливістю суб'єктної частини інформаційної інфраструктури є те, що процес інформатизації сформував у суспільстві особливу сферу діяльності – інформаційну індустрію.

Інформаційна індустрія – широкомасштабне виробництво інформаційних товарів і послуг на базі інформаційних технологій.

Характеризуючи інформаційну інфраструктуру вітчизняного інформаційного середовища та її можливості можна зробити висновок, що вона відповідає сучасному стану становлення ринкових відносин в Україні. Домінуючими у ній виступають засоби масової комунікації, насамперед масмедійні засоби: преса, телебачення, радіо, мережа Інтернет. Основною особливістю вітчизняних масмедіа, як суб'єктів інформаційної інфраструктури, є концентрація їх під владою окремих осіб, а також держави, створення потужних об'єднань, т. з. медіа-холдингів.

1.3. Основні характеристики та класифікація інформації

Слово інформація походить від латинського «information» – виклад, роз'яснення, тлумачення, подання, поняття, обізнаність, просвіта. Поняття інформації неодноразово змінювалось, його межі то розширювалися, то звужувалися. Спочатку під цим словом розуміли уявлення, поняття, потім – відомості, передачу повідомлень.

Так, Закон України «Про інформацію» визначає **інформацію** як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Інформацію поділяють за такими видами, як:

– інформація про фізичну особу;
– інформація довідково-енциклопедичного характеру;
– інформація про стан довкілля (екологічна інформація);
– інформація про товар (роботу, послугу);
– науково-технічна інформація;
– податкова інформація;
– правова інформація;
– статистична інформація;
– соціологічна інформація тощо.

Основні характеристики інформації: цільове призначення, обсяг, цінність, повнота, надійність, вірогідність, надмірність, правдивість, доступність, швидкість передавання та переробки інформації.

Цільове призначення інформації – одна з найважливіших її характеристик, оскільки одна і та ж інформація часто використовується з різною метою. Наприклад, одні і ті ж дані можуть бути використані як для аналізу оперативної обстановки, так і для проведення оперативно-пошукових заходів.

Для передачі та обробки інформації важливого значення набуває її ***обсяг***, який в простішому випадку залежить від кількості знаків (символів), що передаються.

Цінність інформації багато в чому визначається як своєчасністю її передачі, ступенем впливу на рішення, що приймається на її основі, так і важливістю самого рішення. Цінність інформації залежить також від ряду інших характеристик інформації: повноти, надійності, вірогідності.

Така характеристика, як ***повнота*** використовується для визначення змісту найбільш істотних параметрів інформації, що передається. Інформація вважається повною, якщо вона відповідає необхідному обсягу. Невідповідність між інформацією, яка вимагається і яка здобута, свідчить або про неповноту, або про надлишок інформації.

За допомогою ***надійності*** характеризується наявність помилок в інформації, що передається. Надійність багато в чому залежить від технічних засобів, що використовуються.

Інформація може відповідати чи неповністю відповідати тому об’єктові, явищу чи процесу, який вона відображає. Для визначення ступеня відповідності використовують характеристику, яку називають ***вірогідністю***.

Правдивість надходження інформації визначається її вірогідністю, одноразовістю реєстрації, точністю передачі. Якщо інформація проходить три-чотири передавальних ланки, її правдивість знижується до 10% за рахунок старіння і викривлення.

Під ***надмірністю інформації*** розуміється збільшення обсягів даних, що передаються, але які не спричиняють одержання додаткових нових відомостей.

Доступність інформації міститься в тому, що вона знаходиться і накопичується в такому вигляді, що її можна було швидко і легко сприймати і використовувати в управлінні. Мова повідомлення повинна бути зрозумілою

адресату, важливе значення має наочна інформація: графіки, планшети, світлове табло, слайди.

Остання характеристика – ***швидкість передавання та обробки інформації***. Вона залежить від швидкості технічних засобів та систем, що використовуються.

Залежно від способу передачі та сприйняття можна виділити такі види інформації:

– візуальна (передається і сприймається візуальними образами);
– аудіальна (звуками);
– тактильна (відчуттями);
– смакова (запахами);
– машинно-орієнтована (сприймається і обробляється ЕОМ).

За соціальною орієнтацією в науці виділяють масову, особисту і спеціальну інформацію. Якщо масова інформація адресується найширшому колові споживачів, то особиста орієнтована на точно визначеного індивідуума або певну групу осіб. Спеціальна інформація розрахована на спеціалістів. Вона може бути науковою або художньою, технічною або гуманітарною тощо. Спеціальну інформацію часто поділяють за сферами людської діяльності за галузевим принципом. Наприклад: машинобудівна, приладобудівна, енергетична, юридична, медична та ін.

Види інформації, які використовуються в управлінні, класифікуються за наступними ознаками :

– змістом – політична, директивна, правова, науково-технічна, економічна, планова, адміністративна, виробнича, бізнесова, нормативно-довідкова, обліково-бухгалтерська, статистична;
– напрямом руху – вхідна, вихідна;
– характером фіксації – фіксована, нефіксована;
– способом фіксації – документована, звукова, аудивізуальна;
– відношенням до суб’єкта управління – зовнішня, внутрішня;
– ступенем обробки – первинна, довільна, підсумкова;
– ступенем постійності – постійна, перемінна;
– форма надання – літерна, цифрова, кодована;
– можливості обробки – піддається і не піддається обробці;
– насиченості – достатня, недостатня, збиткова;
– правдивості – достовірна, недостовірна.

Політична інформація відображає політику держави щодо бізнесу, соціально-економічного розвитку, різних форм господарювання.

Директивну інформацію виробляють вищі органи, які визначають стратегію господарської діяльності менеджерів і яка слугує основою управління.

Правова інформація визначає статус кожного працівника, його посадове положення і за допомогою якої встановлюють норми господарського і адміністративного права, додержуються законності.

Науково-технічна інформація надає дані про досягнення науки і техніки, для ознайомлення з якою створюються в організаціях відділи або бюро.

Економічна інформація використовується для обґрунтування управлінських рішень і управління економічним розвитком організації. Вона включає розрахунки економічних показників, результати господарської діяльності, аналізу ринку, ціноутворення тощо.

Планова інформація представлена завданнями, технологічними картами, планами за періодами робіт, планами-нарядами тощо.

Адміністративна інформація призначена для оформлення ділових взаємовідносин між організаціями, громадянами і усунення недоліків; оформляється у вигляді наказів, розпоряджень, вказівок, положень.

Виробнича інформація містить оперативні відомості про техніку, технологію виконання планів виробництва і реалізації продукції.

Бізнесова інформація містить відомості про ринкові ціни та їх тенденції, рівень конкуренції, строки і об'єми надходження продукції, сервіс та рекламу, можливості комерційних операцій, підприємництво, комерційний ризик та ін.

Нормативно-довідкова інформація включає норми виробітку і обслуговування, тарифну систему оплати праці, розміри посадових окладів, довідкові дані про техніку, технологію, організацію праці.

Облікова-бухгалтерська інформація дозволяє контролювати хід виробництва і його результати, використання коштів, здобуття прибутку.

Статистична інформація представляє достовірні науково-обґрунтовані відомості, які дозволяють прийняти правильне рішення.

В процесі сприйняття інформації має значення зовнішнє оточення і ситуація. Важливе місце зустрічі осіб, які обмінюються інформацією, характер самої інформації, хто ініціатор зустрічі, присутність інших осіб, шум, музика, все що може впливати і відволікати увагу передаючого і приймаючого інформацію. Сприйняття інформації залежить і від часу, відведеного для учасників обміну. Інформація повинна надходити до своєчасно, а якщо запізнюється, то виникають небажані ситуації, які впливають на організацію виробництва.

1.4. Поняття інформації з обмеженим доступом

За умов жорсткої конкурентної боротьби захист ділової, фінансової, технологічної та іншої інформації від крадіжок, несанкціонованого використання, її зміни чи знищення набуває важливого значення. Комерційні структури, зацікавлені у своїй конкурентоспроможності, насамперед вживають заходів щодо захисту такої інформації, спираючись на відповідні норми чинного законодавства та власну нормативно-правову основу.

Інформація може бути **відкритою** або **з обмеженим доступом**. Якщо відкрита інформація зазвичай не викликає питань щодо її природи, то згідно зі ст. 21 Закону України «Про інформацію» **інформація з обмеженим доступом поділяється на конфіденційну, таємну та службову.**

Конфіденційна інформація – інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень (зг. ЗУ «Про інформацію»).

Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом.

До **таємної інформації** належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі. Віднесення інформації до категорії таємних відомостей, які становлять державну таємницю, і доступ до неї громадян здійснюється відповідно до Закону України «Про інформацію».

До інформації з обмеженим доступом не можуть бути віднесені такі відомості:

– про стан довкілля, якість харчових продуктів і предметів побуту;

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

– про стан здоров'я населення, його життєвий рівень, включаючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

– про факти порушення прав і свобод людини, включаючи інформацію, що міститься в архівних документах колишніх радянських органів державної безпеки, пов'язаних з політичними репресіями, Голодомором 1932-1933 років в Україні та іншими злочинами, вчиненими представниками комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів;

– про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

– інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.

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

Виняток становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої являє загрозу життю і здоров'ю людей.

Відкрита інформація, окрім тієї, доступ до якої не може бути обмежено відповідно до згаданого Закону, здатна переходити до категорії конфіденційної за рішенням її власника або уповноваженої ним особи; відомості, які становлять конфіденційну або таємну інформацію, можуть належати до об'єктів права інтелектуальної власності; інформація, що визнана конфіденційною за рішенням її власника або уповноваженої ним особи, може

також бути віднесена до категорії таємної у випадках, передбачених законодавством.

Закон України «Про інформацію» не містить чіткого розмежування понять конфіденційної інформації та комерційної таємниці. У цьому Законі не встановлено, в чому саме полягає особливість правового режиму інформації комерційного та банківського характеру, але однозначно встановлюється, що такі відомості не можуть бути конфіденційною інформацією.

Найбільший інтерес з погляду захисту комерційних інтересів суб'єкта господарювання викликає комерційна і банківська таємниця.

Неправомірне збирання, розголошення та використання комерційної таємниці є видом недобросовісної конкуренції, який може становити досить серйозну загрозу фінансово-економічній безпеці підприємства.

Інформація щодо діяльності та фінансового стану підприємства, яка стала відомою банку в процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні банківських послуг, і розголошення якої може завдати матеріальної чи моральної шкоди, відповідно до ст. 60 Закону України «Про банки і банківську діяльність» є банківською таємницею.

У питаннях захисту банківської інформації не варто покладатися тільки на державну законодавчу основу, тим більше що остання має багато протиріч і дозволяє по-різному трактувати положення окремих законодавчих актів. Крім того, застосовувати деякі положення законів можна лише спираючись на нормативну основу самого банку.

Велику увагу треба також приділити інформації, яку отримують сторонні особи. Існує поняття інсайдерської інформації, тобто інформації, якою володіють інсайдери – особи, які не працюють на підприємстві, але володіють закритою інформацією про це підприємство. Так, інсайдерами є колишні топ-менеджери – особи, які обіймали керівну посаду на підприємстві (начальник відділу, головний бухгалтер, заступник директора тощо), акціонери, ділові партнери, співробітники юридичних, аудиторських і консалтингових фірм, які надають послуги вашому підприємству.

Окремо регулюється доступ до інформації в автоматизованих системах. Так, згідно зі ст. 4 (Доступ до інформації в системі) Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», доступ до інформації, перелік користувачів та їх повноваження стосовно цієї інформації визначаються власником інформації.

Для належного захисту інформації необхідно обмежити до неї доступ. Обмеження доступу полягає у зменшенні кола осіб, яким відома закрита інформація. Йдеться не лише про встановлення всіляких комп'ютерних паролів, замикання документів у сейфі та знищення чернеток.

Організація системи захисту інформації починається з визначення переліку відомостей, які є комерційною таємницею та конфіденційною інформацією. Керівник підприємства має затвердити наказом Положення про комерційну таємницю та про конфіденційну інформацію на підприємстві, в якому надати перелік таких відомостей і зазначити, що нерозголошення комерційної таємниці та конфіденційної інформації входить до трудових

обов’язків працівників, та визначити відповідальність за невиконання цих обов’язків.

1.5. Інформаційні системи: сутність та класифікація

Інформаційна система – це організаційно впорядкована сукупність інформаційних ресурсів, технічних засобів, технологій, що реалізують інформаційні процеси в традиційному або автоматизованому режимі для задоволення інформаційних потреб користувачів.

З позиції ділового бачення, **інформаційна система** – це сукупність інформації, апаратно-програмних і технологічних засобів телекомунікацій, баз та банків даних, методів процедур оброблення даних, персоналу управління, які організовують процес збирання, передавання, оброблення і накопичування інформації, готування і прийняття ефективних управлінських рішень.

З технічної точки зору **інформаційна система** може бути визначена як набір взаємозалежних компонентів, що збирають, обробляють, зберігають і розподіляють інформацію, щоб підтримувати процес прийняття управлінського рішень і управління організацією в цілому.

Основні завдання інформаційної системи:

– збір інформації з різних джерел;

– реєстрування, оброблення та подання інформації, яка характеризує стан виробництва й управління;

– розподіл інформації між керівниками, підрозділами та виконавцями відповідно до їх участі в управлінні.

До основних функцій ІС належать:

– обчислювальна (вчасне та якісне оброблення інформації в усіх аспектах, які забезпечують функціонування системи управління);

– відстежувальна (відстежування необхідної для управління зовнішньої і внутрішньої інформації);

– запам’ятовувальна (забезпечення постійного накопичення, система збереження і відновлення всієї необхідної інформації);

– комунікаційна (забезпечення передавання необхідної інформації в задані пункти);

– інформаційна (реалізування швидкого доступу, пошуку та подання необхідної інформації);

– регулювальна (здійснення інформаційного впливу на управління та його рівні у випадку відхилень фактичних значень від заданих);

– оптимізаційна (забезпечення оптимальних розрахунків у міру зміни критеріїв та умов функціонування об’єкта управління);

– прогнозування (визначення основних тенденцій, закономірностей і показників розвитку об’єкта управління);

– аналітична (визначення основних показників техніко-економічної діяльності об'єкта управління);

– документувальна (забезпечення отримання всіх обліково-звітних, та інших форм документів).

Інформаційні системи класифікують за рядом характерних ознак.

***За рівнем у системі державного управління*:** територіальні і галузеві; міжгалузеві; підприємств.

Державні інформаційні системи призначені для вирішення найважливіших народногосподарських проблем країни на основі використання обчислювальних комплексів та економіко-математичних методів у них складають перспективні та поточні плани розвитку країни, ведуть облік результатів та регулюють діяльність окремих ланцюгів народного господарства, розробляють державний бюджет та контролюють його виконання тощо.

Територіальні (регіональні) інформаційні системи призначені для управління адміністративно-територіальними регіонами. Сюди належать інформаційні системи області, міста, району. Ці системи виконують роботи з обробки інформації, яка необхідна для реалізації функцій управління регіоном, формування звітності й видачі оперативних даних місцевим і керівним державним та господарським органам.

Міжгалузеві інформаційні системи є спеціалізованими системами функціональних органів управління національною економікою (планових, фінансових, статистичних та інших).

Такі інформаційні системи забезпечують розробку економічних і господарських прогнозів, державного бюджету, здійснюють контроль за результатами та регулювання звітності всіх ланок народного господарства, а також контроль наявності і розподілу ресурсів.

Інформаційні системи управління підприємствами або виробничими об'єднаннями – це системи із застосуванням сучасних засобів автоматизованої обробки даних, економіко-математичних та інших методів для регулярного розв'язування завдань управління виробничо-господарською діяльністю підприємства.

Галузеві або відомчі інформаційні системи управління призначені для управління підвідомчими підприємствами та організаціями. Галузеві ІС діють у промисловості та в сільському господарстві, будівництві, на транспорті та ін. У них розв'язуються завдання інформаційного обслуговування апарату управління відповідних міністерств і відомств.

Створення інтегрованих інформаційних систем дає змогу забезпечити комплексну автоматизацію управління на всіх рівнях. Вона розглядається як ієрархічно організований комплекс організаційних методів, технічних, програмних, алгоритмічних та інформаційних засобів, які мають модульну структуру і забезпечують наскрізне узгоджене управління матеріальними та інформаційними потоками об'єкта управління. Серед інтегрованих інформаційних систем найчастіше виділяють багаторівневі ІС з інтеграцією за рівнями управління (підприємство-об'єднання, об'єднання-галузь тощо), за рівнями планування, за рівнями обліку (бухгалтерський-податковий-статистичний-управлінський) та ін.

За рівнем інтелектуалізації: інформаційно-довідкові; інформаційно-пошукові; підтримки прийняття управлінських рішень; з використанням баз знань; експертні системи.

Інформаційно-пошукові системи призначені для нагромадження та пошуку за певними критеріями документів та даних.

В *інформаційно-довідкових системах* за результатами пошуку обчислюють значення арифметичних функцій.

Документальні ІС використовуються для обробки документів, публікацій, звітів, розпоряджень тощо. Споживачем результатів пошуку виступає, як правило, кінцевий користувач.

Фактографічні системи оброблюють спеціальні фактичні відомості, що являють собою організовану сукупність формалізованих записів даних. Фактографічні системи оперують фактами (даними) різних типів, що пов'язані в системі в більш чи менш складні структури.

Інтелектуальні системи – це такі комп'ютерні системи, які поєднують моделювання і можливість умовиводів. До їх складу входять системи підтримки прийняття рішень, управлінські інформаційні системи, системи засновані на знаннях. Результатом використання цих систем є отримання, оцінка, аналіз, об'єднання і узгодженість різноманітних елементів інформації.

Інформаційно-управлінські системи (ІУС) являють собою організаційно-технічні системи, які забезпечують вироблення рішення на основі автоматизації інформаційних процесів у сфері управління. ІУС призначені для забезпечення керівників вищого та середнього рівня інформацією. Для систем, заснованих на знаннях характерним є застосування штучного інтелекту для того щоб висувати гіпотези і робити розумні висновки. Штучний інтелект пропонує представлення знань (фактів, правил) у пам'яті комп'ютера поряд з деякою можливістю робити висновки і навчатися. Великий прогрес у використанні штучного інтелекту був досягнутий для вирішення структурних проблем, які вимагають від людей високого інтелекту, наприклад, гра в шахи, переклад з однієї мови на іншу.

***За ступенем централізації оброблення інформації*:** централізовані і децентралізовані.

Централізовані ІС – накопичення і оброблення інформації здійснюється в єдиному центрі. Доступ інформаційних ресурсів ІС може здійснюватись віддалено.

Децентралізовані ІС побудовані за автономним принципом. Кожна ІС певного рівня обслуговує певне коло користувачів.

***За принципом інтегрування*:** багаторівневі з інтеграцією за рівнями управління та функціями управління; одноріневі.

За видами процесів: для наукових досліджень; для автоматизованого проектування; організаційного управління; управління виробничими процесами; управління технологічними процесами; навчальні.

***За сферою діяльності*:** культурологічні; владні; науково-технічні; соціальні; фінансово-економічні; міжнародних організацій.

За режимом оброблення інформації: в режимі реального часу; в автономному режимі.

За ступенем автоматизапції перетворення економічної інформації.

До *немеханізованих систем* належать ті, в яких обробку обліково-економічної інформації здійснюють вручну, а найпростішу обчислювальну техніку, зокрема арифмометри і калькулятори, використовують в індивідуальному порядку для окремих обчислень.

До *напівмеханізованих інформаційних систем* належать такі, в яких обробку обліково-економічної інформації виконували за допомогою обчислювальних машин з ручним введенням даних (клавішні машини), котрі були в експлуатації в машинно-рахункових бюро.

До *механізованих систем* належать такі, в яких обробку обліково-економічної інформації виконували за допомогою обчислювальних машин з механізованим введенням даних, зафіксованих на машинних носіях.

До *автоматизованих інформаційних систем* належать такі, в яких фіксацію, збір та обробку обліково-економічної інформації виконують за допомогою електронних обчислювальних машин, технічних засобів зв’язку, периферійного електронного обладнання, де частина функцій (підсистем) управління або обробки даних здійснюється автоматично, а частину здійснює людина. В автоматичних інформаційних системах усі функції управління й обробки даних здійснюють технічними засобами без участі людини (наприклад, автоматичне управління технологічними процесами).

ТЕМА 2
ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

2.1. Сутність інформаційної безпеки підприємства. Принципи інформаційної безпеки підприємства

2.2. Характеристика загроз інформаційній безпеці підприємства

2.3. Методи, заходи та засоби забезпечення інформаційної безпеки підприємства

2.1. Сутність інформаційної безпеки. Принципи інформаційної безпеки підприємства

Давно відомо, що інформація може бути справжнім скарбом. Саме тому часто багато зусиль витрачається як на охорону інформації, так і на добування її.

Інформація з погляду безпеки – це дані, відомості, документи, які повинні бути захищеними через їх важливість для суб'єкта господарювання від незаконного втручання, розкриття чи розголошення.

Основу правового статусу інформації визначає Закон України «Про інформацію». Інформацію у ст. 1 вищезазначеного Закону визначено як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

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

Крім того, під інформаційною безпекою розуміють захищеність інформації та її підтримуючої інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може з'явитися нанесення збитку самій інформації, її власникам або підтримуючій інфраструктурі.

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

Основними принципами інформаційної безпеки є:

– забезпечення цілісності і збереження даних, тобто надійне їх зберігання в неспотвореному вигляді;

– дотримання конфіденційності інформації (її недоступність для тих користувачів, які не мають відповідних прав);

– доступність інформації для всіх авторизованих користувачів за умови контролю за всіма процесами використання ними отриманої інформації;

– безперешкодний доступ до інформації в будь-який момент, коли вона буде необхідна.

Ці принципи неможливо реалізувати без особливої інтегрованої системи інформаційної безпеки, що виконує **наступні функції:**

– вироблення політики інформаційної безпеки;

– аналіз ризиків (тобто ситуацій, в яких може бути порушена нормальна робота інформаційної системи, а також втрачені або розсекречені дані);

– планування заходів щодо забезпечення інформаційної безпеки;

– планування дій в надзвичайних ситуаціях;

– вибір технічних засобів забезпечення інформаційної безпеки.

2.2.Характеристика загроз інформаційній безпеці підприємства

Інформаційний розвиток, що зумовив кардинальні зміни в економіці, праві, соціальному житті одночасно сприяв формуванню нових видів загроз у діяльності підприємств.

Забезпечення збереження інформації необхідно починати з визначення системи загроз, тобто негативних процесів, які сприяють витоку інформації. Для успішного захисту інформації необхідно знати весь перелік загроз безпеки. Якщо розробник має повний список загроз, то він зможе вибрати необхідні і застосувати потрібні для їх усунення засоби захисту.

В сучасному інформаційному середовищі існують два види загроз:

– інформаційні, які надходять від власне інформації та її технологій;

– загрози самій інформації, пов’язаних з різного роду посяганнями на інформацію та її об’єкти.

Інформаційні загрози – наявність в інформаційному середовищі шкідливої або небезпечної для його суб’єктів інформації, інформаційної продукції та технологій, здатних негативно впливати на їх стан, поведінку та взаємовідносини.

Загрози інформації – дії, пов’язані з несанкціонованим доступом до об’єктів інформації або спрямовані на її викрадення, знищення, модифікацію, копіювання, блокування чи іншим чином позбавлення власника інформації переваг від її використання.

Інформаційні загрози:

– загроза інформаційної залежності;

– наявні, практично безмежні обсяги необ’єктивної інформації, що наповнюють інформаційне середовище;

–дискредитація суб’єктів (поширення негативної неправдивої інформації про суб’єктів, маніпулювання індивідуальною та колективною свідомістю працівників, клієнтів, акціонерів, споживачів або просто громадян, дезінформація різних осіб у взаємовідносинах з суб’єктами, поширення негативних чуток про останніх, здійснення актів інформаційного тероризму та провокування інформаційних конфліктів, втягування суб’єктів в інформаційну війну).

– промислове шпигунство, яке охоплює практично всі складові ринкової економіки. Промислове шпигунство передбачає отримання інформації, яка тим чи іншим чином характеризує відповідні технології, плани, розробки, ідеї, рішення, що є цікавими для конкурентів. Не обов’язково, щоб інформація була таємною або конфіденційною, головне, щоб вона була корисною для конкурента або іншого суб’єкта;

– кібертероризм. Особлива небезпечність кібертероризму полягає в

тому, що він одночасно несе в собі загрозу інформаційним ресурсам суб'єктів підприємництва і загрозу їх іміджу, суспільній оцінці їх діяльності.

Інформаційні ризики за своїм походженням поділяються на три категорії:

– ризики, пов'язані з втратою (витоком, руйнуванням, знищенням) інформації. Особливо це небезпечно, коли існує ризик втрати такої важливої для діяльності суб'єктів підприємництва інформації, як банківська та комерційна таємниця, або іншої інформації з обмеженим доступом;

– ризики, пов'язані з формуванням інформаційного ресурсу (використання неповної, неправдивої інформації, відсутність необхідної інформації, дезінформація);

– ризики, пов'язані з інформаційним впливом на діяльність суб'єктів підприємництва (поширення неправдивої та негативної інформації, інформаційно-психологічний вплив на працівників, клієнтів та акціонерів, інформаційний тероризм).

Основні загрози інформації і нормального функціонування інформаційної системи:

– розголошення інформації, просочування конфіденційної інформації;

– викрадення інформації;

– знищення інформації;

– модифікація інформації;

– несанкціоноване використання інформаційних ресурсів;

– помилкове використання інформаційних ресурсів;

– відмова від інформації;

– порушення інформаційного обслуговування.

Розголошення інформації розуміється як протиправні умисні чи необережні дії посадових або інших осіб, які призвели до несанкціонованого, без службової необхідності, оголошення (поширення) відомостей щодо яких встановлено відповідний порядок їх розкриття. Воно може здійснюватись шляхом повідомлення, передачі, пересилання, публікації, втрати чи іншим шляхом оприлюднення зазначених відомостей.

Просочування конфіденційної інформації – це її безконтрольний вихід за межі інформаційної системи або через коло осіб, яким вона була довірена за видом служби або стала відома в процесі роботи. Цей витік може бути наслідком:

– розголошування конфіденційної інформації;

– витоку інформації різними, переважно технічними каналами;

– несанкціонованого доступу до конфіденційної інформації різними способами.

Розголошування інформації, що призвело до ознайомлення з нею осіб, не допущених до цих відомостей, можна кваліфікувати як умисні або необережні дії посадових осіб і користувачів, яким ці відомості були довірені у зв'язку зі службовою потребою.

Можливий безконтрольний витік конфіденційної інформації візуально-оптичним, акустичним, електромагнітним та іншими каналами.

Несанкціонований доступ – це протиправне навмисне оволодіння конфіденційною інформацією особою, яка не має права доступу до відомостей, що охороняються. Найпоширенішими напрямами несанкціонованого доступу до інформації є:

– перехоплення електронних випромінювань;

– примусове електромагнітне опромінювання (підсвічування) ліній зв'язку з метою отримання паразитної модуляції;

– застосування підслуховуючих пристроїв (жучків);

– дистанційне фотографування;

– перехоплення акустичних випромінювань і відновлення тексту принтера;

– зчитування залишкової інформації в пам'яті системи після виконання санкціонованих запитів;

– копіювання носіїв інформації з подоланням заходів захисту;

– маскування під зареєстрованого користувача;

– маскування під запити системи;

– використання програмних пасток;

– використання недоліків мов програмування і операційних систем;

– незаконне підключення до апаратури і ліній зв'язку спеціально розроблених апаратних засобів, що забезпечують доступ інформації;

– зловмисне виведення з ладу механізмів захисту;

– розшифровування спеціальними програмами зашифрованої інформації.

Викраденням інформації є таємне вилучення носіїв інформації (документів, електронних носіїв, відео- та аудиозаписів) з метою подальшого їх використання іншою особою чи передачі їх такій особі.

Знищенням є приведення носіїв інформації (документів, електронних носіїв, аудіо-, відеозаписів та інших носіїв, що мають матеріальний характер) в стан непридатний для їх подальшого використання або ж неможливості використання інформації, яка на них зберігалась.

Модифікацією інформації є внесення змін до змісту інформації, яка містилась на певних носіях або ж до самих носіїв (комп'ютерних програм) в результаті чого використання даної інформації стає неможливим взагалі чи така інформація вимагає суттєвого уточнення та аналізу.

Незаконне використання інформації означає використання певних даних, знань, технологій, які на праві власності належать певній юридичній чи фізичній особі без її згоди або з порушенням встановленого порядку їх використання особами, яким така інформація відома у зв'язку з їх службовою чи іншою діяльністю.

Несанкціонованим буде також доступ до інформації з порушенням встановлених правил доступу до неї.

Помилкове використання інформаційних ресурсів може призвести до знищення, розкриття або компрометації цих ресурсів. Така загроза є переважно наслідком помилок програмного забезпечення інформаційної системи.

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

Порушення інформаційного обслуговування полягає у затримці надання ресурсів абонентові, що може призвести до тяжких наслідків. Наприклад, відсутність в абонента даних, необхідних для прийняття рішень, може бути причиною його нераціональних або неоптимальних дій.

Існує безліч класифікацій видів загроз за принципами і характером їх дії на систему, щодо використовуваних засобах , за цілями атаки тощо.

Загрози інформаційній безпеці поділяються на **випадкові і навмисні**.

Джерелом **випадкових** можуть бути аварійні ситуації через стихійні лиха і відключення електроживлення, відмови і збої апаратури, помилки в програмному забезпеченні, помилки в роботі обслуговуючого персоналу і користувачів, перешкоди в лініях зв'язку через впливи зовнішнього середовища.

Навмисні загрози пов'язані з цілеспрямованими діями порушника, яким можуть виступати службовці, відвідувачі, конкуренти, працівники.

Навмисні загрози в свою чергу поділяються на **пасивні і активні**.

Пасивні загрози носять характер перехоплення або моніторингу переданої інформації і не пов'язані з якою-небудь зміною інформації. Їх можна умовно розділити на дві групи: розкриття вмісту повідомлення (телефонна розмова, електронна пошта) і аналіз потоку даних.

Пасивні порушення виявити дуже важко, але їх цілком реально попередити. **Активні** загрози пов'язані зі зміною потоку даних або зі створенням фальшивих потоків

Класифікація загроз інформаційній безпеці за засобами впливу на систему.

За засобами впливу розрізняють три основні класи загроз:

1. Втручання людини в роботу обчислювальної системи. До цього класу належать організаційні засоби порушення безпеки (крадіжка носіїв інформації, несанкціонований доступ до пристроїв зберігання і обробки інформації, псування устаткування тощо.) І здійснення порушником несанкціонованого доступу до програмних компонентів системи (всі способи несанкціонованого проникнення в систему, а також способи отримання користувачем-порушником незаконних прав доступу). Заходи, що протистоять таким загрозам, носять організаційний характер, а також включають в себе вдосконалення систем розмежування доступу і системи виявлення спроб атак (наприклад, спроб підбору паролів).

2. Апаратурно-технічне втручання в роботу обчислювальної системи. Мається на увазі порушення безпеки та цілісності інформації за допомогою технічних засобів, наприклад, отримання інформації по електромагнітному випромінюванні пристроїв, електромагнітні впливи на канали передачі інформації та інші методи. Захист від таких загроз, крім організаційних заходів, передбачає відповідні апаратні і програмні заходи.

3. Руйнівний вплив на програмні компоненти системи за допомогою програмних засобів. Такі засоби називаються руйнівними програмним засобами

(РПС). До них відносяться комп'ютерні віруси, троянські коні, засоби проникнення у віддалені системи з використанням локальних і глобальних мереж. Засоби боротьби з подібними атаками складаються з програмно-і (рідше) апаратно-реалізованих систем захисту.

Загрози інформаційній безпеці поділяються на внутрішні і зовнішні.

Внутрішні загрози:

– некваліфікована політика щодо організації інформаційних технологій та управління безпекою підприємства;

– відсутність належної кваліфікації персоналу;

– навмисні і ненавмисні дії персоналу, що призводять до порушення інформаційної безпеки;

– техногенні аварії, пожежі тощо.

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

– основний персонал (користувачі, програмісти, розробники);

– представники служби захисту інформації;

– допоміжний персонал (прибиральники, охорона);

– технічний персонал.

***Зовнішні загрози*:**

– негативні дії недобросовісних конкурентів і державних структур;

– навмисні і ненавмисні дії зацікавлених структур і фізичних осіб (збір інформації, шантаж, погрози фізичного впливу тощо);

– витік конфіденційної інформації із носіїв інформації та каналів зв'язку;

– несанкціоноване проникнення на об'єкт захисту;

– несанкціонований доступ до носіїв інформації і каналів зв'язку з метою знищення, викривлення, викрадення, блокування інформації;

– стихійні лиха та інші форс-мажорні обставини;

– неавмисні і ненавмисні дії постачальників послуг в сфері забезпечення безпеки, постачальників програмних продуктів тощо.

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

– кримінальні структури;

– потенційні злочинці і хакери;

– нечесні партнери;

– технічний персонал постачальників послуг тощо.

2.3. Методи та засоби забезпечення інформаційної безпеки підприємства

Для запобігання загрозам інформаційній безпеці та їх усунення використовують правові, програмно-технічні та організаційно-економічні методи.

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

Програмно-технічні методи передбачають:

– запобігання витоку інформації;

– усунення можливості несанкціонованого доступу до інформації;

– запобігання впливам, які призводять до знищення, руйнування, переключення інформації, або збоям чи відмовам у функціонуванні засобів інформатизації;

– виявлення вмонтованих пристроїв;

– запобігання перехопленню інформації технічними засобами;

– використання криптографічних засобів захисту інформації під час передачі каналами зв'язку.

Організаційно-економічні методи передбачають:

– формування і забезпечення функціонування систем захисту секретної і конфіденційної інформації;

– сертифікацію цих систем відповідно до вимог інформаційної безпеки;

– ліцензування діяльності у сфері інформаційної безпеки;

– стандартизацію способів і засобів захисту інформації;

– контроль за діями персоналу в захищених інформаційних системах.

Крім цих груп методів використовують ще й такі **методи забезпечення інформаційної безпеки:**

– ідентифікація та аутентифікації користувачів (так званий комплекс 3А);

– шифрування інформації, що зберігається на комп'ютерах і передається по мережах;

– міжмережеві екрани;

– віртуальні приватні мережі;

– засоби контентної фільтрації;

– інструменти перевірки цілісності вмісту дисків;

– протидія атакам шкідливих програм;

– системи виявлення вразливостей мереж і аналізатори мережевих атак;

– перешкода;

– регламентація;

– примус;

– спонука;

– мотивація, економічне стимулювання і психологічна підтримка діяльності персоналу.

Кожен з перерахованих засобів може використовуватись як самостійно, так і в інтеграції з іншими.

«Комплекс 3А» включає аутентифікацію (або ідентифікацію), авторизацію та адміністрування. Ідентифікація та авторизація – це ключові елементи інформаційної безпеки. При спробі доступу до інформаційних активів функція ідентифікації дає відповідь на питання: чи ви є авторизованим користувачем мережі?. Функція авторизації відповідає за те, до яких ресурсів конкретний користувач має доступ. Функція адміністрування полягає у наділенні користувача певними ідентифікаційними особливостями в рамках даної мережі і визначенні обсягу допустимих для нього дій.

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

Міжмережевий екран являє собою систему або комбінацію систем, що утворить між двома чи більш мережами захисний бар'єр, що оберігає від несанкціонованого потрапляння в мережу або виходу з неї пакетів даних.

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

Говорячи про криптографію і міжмережеві екрані, слід згадати про захищені *віртуальні приватні мережі* (Virtual Private Network – VPN). Їх використання дозволяє вирішити проблеми конфіденційності і цілісності даних при їх передачі по відкритим комунікаційних каналам. Використання VPN можна звести до вирішення трьох основних завдань:

1. Захист інформаційних потоків між різними офісами компанії (шифрування інформації проводиться тільки на виході у зовнішню мережу).
2. Захищений доступ віддалених користувачів мережі до інформаційних ресурсів компанії, як правило, здійснюваний через Internet.
3. Захист інформаційних потоків між окремими додатками всередині корпоративних мереж (цей аспект також дуже важливий, оскільки більшість атак здійснюється з внутрішніх мереж).

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

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

Всі зміни на робочій станції або на сервері можуть бути відслідковані адміністратором мережі або іншим авторизованим користувачем завдяки

технології перевірки цілісності вмісту жорсткого диска (integrity checking). Це дозволяє виявляти будь-які дії з файлами (зміна, видалення або ж просто відкриття) і ідентифікувати активність вірусів, несанкціонований доступ або крадіжку даних авторизованими користувачами. Контроль здійснюється на основі аналізу контрольних сум файлів (CRC сум).

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

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

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

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

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

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

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

Існують такі засоби забезпечення інформаційної безпеки:

– технічні, які поділяють на апаратні та фізичні;
– програмні;
– організаційні;
– правові;

– морально-етичні.

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

Фізичні засоби – це різні інженерні пристрої і споруди, що перешкоджають фізичному проникненню зловмисників на об'єкти захисту і здійснюють захист персоналу (особисті засоби безпеки), матеріальних засобів і фінансів, інформації від протиправних дій (замки на дверях, фати на вікнах, засоби електронної охоронної сигналізації).

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

Організаційні засоби здійснюють регламентацію виробничої діяльності в ІС і взаємин виконавців на нормативно-правовій основі так, що розголошування, витік і несанкціонований доступ до конфіденційної інформації стають неможливими або досить складними за рахунок проведення організаційних заходів. Комплекс цих заходів реалізує група інформаційної безпеки, але має бути під контролем першого керівника.

Законодавчі засоби захисту визначаються законодавчими актами країни, якими регламентуються правила користування, опрацювання і передавання інформації обмеженого доступу і встановлюють заходи відповідальності за порушення цих правил.

Морально-етичні засоби захисту – різні норми поведінки, які традиційно склалися раніше, формуються у спосіб розповсюдження ІС і ІТ в країні і світі або спеціально розробляються. Вони можуть бути неписані (чесність) або оформлені в якесь зведення (статут) правил чи розпоряджень.

ТЕМА 3
ОСНОВИ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

3.1. Структура інформаційної безпеки підприємства

Інформація – умова ефективного здійснення підприємницької діяльності, вона використовується як засіб впливу на ринкову ситуацію, взаємовідносини суб'єктів, інформація має комерційну цінність і може виступати окремим видом економічної діяльності. Інформація є основою знань, тобто інтелектуального потенціалу підприємств, які необхідно захищати.

Інформаційна безпека підприємства – стан інформаційної роботи підприємства, за якого забезпечується ефективне інформаційне супроводження його діяльності, надійний захист інформаційного ресурсу та результативна протидія негативному інформаційно-психологічному впливу на нього.

Структуру інформаційної безпеки підприємства складають три складові (рис. 3.1).

Рис. 3.1. Структура інформаційної безпеки підприємства

Враховуючи динамічний характер сучасного інформаційного простору, такий підхід до розуміння суті та змісту інформаційної безпеки забезпечує підприємствам необхідний рівень живучості у їх конкурентній боротьбі, більш оптимальну поведінку у взаємовідносинах поміж собою, іншими організаціями та інституціями. Інформаційна безпека у такому розумінні виступає формою існування підприємств у інформаційному середовищі.

Метою інформаційної безпеки у такому випадку є виключення можливості втрати підприємствами свого інформаційного ресурсу чи його руйнування, заподіяння шкоди їх іміджу, а також формування умов для ефективної діяльності і отримання прибутку. Критерієм же ефективності інформаційної безпеки є стабільність оцінки діяльності суб'єктів підприємництва на ринку та позитивні перспективи їх розвитку.

Очевидно, що досягнення визначеної мети інформаційної безпеки має забезпечуватись **виконанням певних завдань**:

– організація відповідного режиму функціонування інформації в діяльності підприємства;

– формування, необхідного для забезпечення ефективної діяльності підприємства, інформаційного ресурсу;

– своєчасне виявлення загроз інформаційному ресурсу та іміджу підприємства, його інформаційним відносинам;

– оперативне реагування підприємства на зміни та порушення умов інформаційних відносин, спроби посягань на його інформаційні ресурси та імідж;

– підготовка персоналу підприємства з питань інформаційної безпеки;

– оптимізація заходів та витрат пов'язаних з забезпеченням інформаційної безпеки підприємницької діяльності.

Зазначені завдання повинні бути інтегровані у повсякденну діяльність підприємства шляхом планової роботи як спеціальних підрозділів інформаційної безпеки, так і всіх інших, що входять до складу організаційної структури суб'єкта.

3.2. Принципи організації інформаційної безпеки на підприємстві

Основні принципи організації інформаційної безпеки на підприємстві:

– *законність* – заходи, що виконуються в межах організації та здійснення інформаційної безпеки мають вкладатись в межі чинного законодавства, не порушувати права та свободи громадян, законні інтереси інших суб'єктів та держави;

– *самостійність та відповідальність* – заходи інформаційної безпеки обираються підприємством самостійно, в межах своїх можливостей і повинні бути адекватними загрозам його інформаційній безпеці; за результати вжитих заходів відповідальність покладається на підприємство та уповноважених ним на проведення таких заходів осіб;

– *компетентність* – виконання заходів інформаційної безпеки має здійснюватись грамотно, на високому професійному рівні, підготовленими для цього фахівцями;

– *економічна доцільність* – витрати на організацію та виконання заходів інформаційної безпеки повинні бути адекватними її ефективності, не завдавати шкоди економічному стану підприємства;

– *цілеспрямованість* – заходи інформаційної безпеки повинні здійснюватись у строгій відповідності основним завданням і напрямам діяльності підприємства;

– *конфіденційність* – переважна сукупність заходів інформаційної безпеки проводиться на конфіденційній основі, інформування про їх проведення та результати, здійснюється лише обмеженому колу осіб.

Надійність та ефективність інформаційної безпеки підприємства визначається через її відповідність встановленим вимогам:

– *безперервність забезпечення інформаційної безпеки* – заходи інформаційної безпеки проводяться з початком її організації і продовжуються протягом всього часу існування підприємства, посилюючись та послаблюючись в окремих ситуаціях, але без їх припинення;

– *плановість інформаційної безпеки* – встановлення відповідного порядку застосування заходів інформаційної безпеки, який би забезпечував запобіжний характер їх впливу на виникнення небезпек і загроз;

– *конкретність інформаційної безпеки* – заходами безпеки повинні бути охоплені конкретні об'єкти та дії підприємства; заходи безпеки повинні бути пов'язані з конкретними операціями, угодами, відносинами, які здійснюються на даний час підприємством;

– *активність інформаційної безпеки* – в арсеналі заходів інформаційної безпеки повинні бути як такі, що забезпечують захист інформаційного ресурсу та іміджу підприємства, так і ті, які спрямовуються на протидію заходом негативного впливу та розкриття їх джерел;

– *комплексність інформаційної безпеки* – передбачає необхідність застосування у забезпеченні безпеки різних форм, методів, засобів, заходів щодо різних видів інформації та інформаційних відносин.

3.3. Види інформаційної безпеки підприємства

У практиці забезпечення інформаційної безпеки суттєве значення має визначення її видів. Особливо це необхідно з точки зору організації інформаційної безпеки в діяльності підприємств.

Види інформаційної безпеки підприємства:

– комп'ютерна безпека;
– інформаційно-психологічна безпека;
– комунікаційна безпека;
– документаційна безпека.

Комп'ютерна безпека передбачає: захист засобів комп'ютеризації, комп'ютерних технологій і інформації, що знаходиться на електронних носіях; отримання необхідної підприємству інформації із глобального інформаційного простору (мережі Інтернет) для формування його інформаційного ресурсу; протидія інформаційним загрозам в середовищі електронної інформації (комп'ютерні віруси, шкідливі програми, комп'ютерний тероризм тощо).

Інформаційно-психологічна безпека. Основними напрямами забезпечення інформаційної безпеки є організація захисту інтелектуальної власності, режиму використання інформації працівниками та іншими особами у процесі інформаційних відносин; збереження інформаційного здоров'я працівників суб'єктів підприємництва в умовах інформатизації виробництва; розробка технологій отримання знаннєвої інформації (наукові дослідження, конференції, семінари, курси, сімпозіуми і т. п.) для формування інформаційного ресурсу підприємства; протидія технологіям маніпулювання інформацією, індивідуальною та колективною свідомістю.

Комунікаційна безпека включає захист інформації в процесі взаємообміну (електронна пошта, мобільний зв'язок) та ділового спілкування

(зустрічі, перемовини); проведення заходів пропаганди, контр-пропаганди та агітації в інформаційному середовищі підприємства; протидія поширенню негативної інформації засобами масової комунікації.

Документаційна безпека спрямована, перш за все, на захист документованої інформації та її носіїв, насамперед через запровадження надійної системи загального і спеціального діловодства, розробки нормативних документів з питань інформаційної безпеки; запровадження технологій отримання необхідних даних з різного роду документів (правових актів, звітів, звичайних публікацій, виступів, описів і т. п.) для формування інформаційного ресурсу суб'єктів підприємництва; документальне супроводження протидії інформаційним загрозам та інформаційно-психологічному впливу щодо суб'єктів підприємництва, їх діяльності та персоналу (документування фактів порушення інформаційного режиму, поширення неправдивої інформації чи маніпулювання нею, документальне спростування негативної інформації, документи щодо вимог відшкодування моральної шкоди і т. і.).

3.4. Особливості організації інформаційної безпеки на підприємстві

Підвалинами успіху інформаційної безпеки є грамотна її організація в діяльності підприємства. На жаль, саме організація на сьогодні є одним із найбільш слабких місць у забезпеченні інформаційної безпеки підприємств.

Грамотно організована інформаційна безпека є запорукою успіху підприємства у його інформаційних відносинах і діяльності взагалі. Організація інформаційної безпеки є елементом управління безпекою підприємства. Тому цим питанням має опікуватись насамперед його керівництво. Так, з питань організації інформаційної безпеки керівники підприємств мають визначити мету безпеки, її основні завдання та напрями зосередження основних зусиль; створити сприятливі умови для діяльності сил інформаційної безпеки відповідно до функцій покладених на неї; забезпечувати контроль ефективності функціонування системи інформаційної безпеки. Безпосереднім організатором інформаційної безпеки є керівник підрозділу безпеки підприємства, а там де він відсутній – сам керівник підприємства.

Аналіз практики забезпечення інформаційної безпеки в підприємницькій діяльності показує, що питанням її організації не надається необхідного значення, в більшості випадків керівники підрозділів безпеки ними володіють майже на примітивному рівні. Процес організації практично відсутній у керівництві інформаційною безпекою суб'єктів підприємництва. Здебільшого організація безпеки зводиться до реакції на негаразди, які виникають у інформаційних відносинах суб'єктів підприємництва. Потенціал, закладений у грамотній організації інформаційної безпеки, не сприймається як перевага в інформаційному середовищі, конкурентній боротьбі, ринкових відносинах взагалі.

Структура процесу організації інформаційної безпеки підприємства (рис. 3.2).

Процес організації інформаційної безпеки підприємства виконується на підставі глибокого вивчення умов та змісту діяльності підприємства, характеру

його взаємовідносин на ринку та поведінки в інформаційному середовищі. Крім того, процесу організації мають передувати вивчення можливостей підприємства щодо забезпечення відповідного рівня інформаційної безпеки та правових умов, в яких здійснює свою діяльність суб'єкт. Процедура та зміст організації інформаційної безпеки обов'язково має бути узгоджена з точкою зору керівника підприємства. Точка зору керівника має бути сформована як його рішення з цього питання.

Важливим в організації інформаційної безпеки суб'єктів підприємництва залишається створення відповідної системи.

Система інформаційної безпеки підприємства – певна сукупність сил, засобів, заходів і технологій, спрямованих на забезпечення високої стійкості підприємства до інформаційних загроз та ефективне інформаційне супроводження його діяльності.

Рис. 3.2. Структура процесу організації інформаційної безпеки підприємства

Основні принципи формування системи інформаційної безпеки:

– *стійкість* – система має ефективно протистояти будь-яким діям, спрямованим на її руйнування чи дестабілізацію функціонування;

– *адаптація* – система має оперативно реагувати на будь-які зміни в інформаційному середовищі та інформаційних відносинах підприємства;

– *трансформація* – система має працювати з різними видами інформації, в різних інформаційних середовищах, в будь-яких комунікаційних мережах без втрати ефективності забезпечення інформаційної безпеки підприємства;

– *відновлення* – система має бути здатною в оптимально короткі терміни відновлювати свою живучість та забезпечувати виконання необхідного обсягу заходів інформаційної безпеки підприємства обмеженим складом сил і засобів;

– *автономність* – система має бути максимально незалежною від зовнішніх джерел та суб'єктів, забезпечувати своє функціонування власними силами та засобами.

Таким чином, враховуючи структуру та зміст завдань інформаційної безпеки, обсяг заходів, які покладаються на неї, можна стверджувати, що вона займає одне із провідних місць у забезпеченні безпеки діяльності підприємства.

В той же час, забезпечення інформаційної безпеки – це досить складний і трудомісткий процес, який вимагає значних фінансових, матеріальних, інтелектуальних зусиль. Останні ж мають спиратись на грамотні, науково обґрунтовані та підтверджені підприємницькою практикою погляди професіоналів, здатних реалізувати визначену певним суб'єктом підприємництва концепцію інформаційної безпеки.

ТЕМА 4
ОСОБЛИВОСТІ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

4.1. Характеристика інформації з обмеженим доступом

4.2. Сутність комерційної таємниці. Перелік відомостей, що не становлять комерційної таємниці

4.3. Організація захисту комерційної таємниці на підприємстві

4.4. Система захисту інформації на підприємстві

4.1. Характеристика інформації з обмеженим доступом

Захист інформації посідає важливе місце у вирішенні проблеми забезпечення інформаційної безпеки будь-якого підприємства. Це пов'язане з недопущенням втрати чи знищення інформації, її модифікації, встановлення безпечного режиму її функціонування у процесі діяльності підприємства.

У діяльності підприємства використовується два види інформації: **відкрита** і **таємна.** Таємна – це насамперед банківська і комерційна таємниця, а також конфіденційна інформація. Тому важливим моментом у захисті інформації буде виступати порядок виділення такої інформації як окремого об'єкту захисту.

Відповідно до вітчизняного законодавства громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаної за власні кошти, або таку, що є предметом їх ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної та встановлюють до неї систему захисту.

Тобто, право встановлювати відповідний режим доступу до інформації мають особи (юридичні та фізичні), які володіють інформацією. За таких умов суб'єкти підприємництва мають право обмежувати доступ до власної інформації, в тому числі і щодо якої вони стали володільцями в результаті її придбання або, яка не є їх власністю, але є предметом їх інтересу (будь-які відомості отримані підприємством в результаті проведення заходів інформаційного забезпечення його діяльності).

Конфіденційна інформація підприємства як вид інформації з обмеженим доступом може мати подвійний характер. З одного боку, це інформація, власниками якої є суб'єкти підприємництва і яка з тих чи інших причин не отримала категорії таємної та інформація про персонал, яка зберігається в особових справах та документах про оплату праці. Якщо перелік відомостей, що становить конфіденційну інформацію суб'єктів підприємництва визначається в тому ж порядку, що і для комерційної таємниці, то зміст конфіденційної інформації про працівників подається у Законі України «Про інформацію» та забезпечується відповідно до Закону України «Про захист персональних даних». Суб'єкти підприємництва зобов'язані забезпечити конфіденційність таких даних, зібраних на своїх працівників при прийомі на роботу та їх звільненні.

Підприємства, здійснюючи господарську діяльність виробляють свою власну інформацію, що може бути для них досить важливою та цінною. При розробці нових технологій виробництва, нової продукції, плануванні розвитку, створюються насичені різноманітними відомостями інформаційні об'єкти, які вимагають надійного захисту. Тому підприємства повинні захищати такі об'єкти шляхом надання їм категорії **комерційної таємниці.**

4.2. Сутність комерційної таємниці. Перелік відомостей, що не становлять комерційної таємниці

Згідно зі ст. 505 ЦК України **комерційною таємницею** є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою і не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть належати до комерційної таємниці.

Отже, **комерційна таємниця** – це відомості технічного, організаційного, комерційного, виробничого та іншого характеру, які є об'єктом інтелектуальної власності, мають комерційну цінність, розголошення яких може завдати шкоди інтересам суб'єкта господарювання.

Відповідно до цивільного законодавства **основними ознаками комерційної таємниці** є:

– комерційна цінність інформації;

– інформація повинна бути невідомою третім особам і до неї немає вільного доступу;

– володілець інформації має вживати відповідних заходів для її охорони і таємності;

– інформація не може бути об'єктом інших таємниць.

Враховуючи, що суб'єкти підприємництва, як власники інформації самостійно визначають зміст своїх таємниць, значення набуває процес формування переліку відомостей, що становлять комерційну таємницю.

З одного боку зазначений перелік повинен надійно захищати цінну для суб'єктів інформацію, а з іншого, не обмежувати їх інформаційну діяльність на ринку.

Склад та обсяг відомостей, які становлять комерційну таємницю підприємства, визначаються його керівником з урахуванням постанови Кабінету Міністрів України «Про перелік відомостей, що не становлять комерційної таємниці» від 9 серпня 1993 р. № 611.

Перелік відомостей, що комерційну таємницю не становлять:

– установчі документи, документи, що дозволяють займатися підприємницькою діяльністю та її окремими видами;

– інформація за всіма встановленими формами державної звітності;

– дані, необхідні для перевірки обчислення і сплати податків та інших обов'язкових платежів;

– відомості про чисельність і склад працівників, їхню заробітну плату в цілому та за професіями й посадами, а також наявність вільних місць;

– документи про сплату податків і обов'язкових платежів;

– інформація про забруднення навколишнього природного середовища, недотримання безпечних умов праці, реалізацію продукції, що завдає шкоди здоров'ю, а також інші порушення законодавства України та розміри заподіяних при цьому збитків;

– документи про платоспроможність;

– відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, спілках та інших організаціях і об'єднаннях, які займаються підприємницькою діяльністю;

– відомості, що відповідно до чинного законодавства підлягають оголошенню. До такої інформації може бути віднесена, зокрема, інформація про випуск акцій підприємством, що пропонуються для відкритого продажу, яка згідно зі статтею 23 Закону України «Про цінні папери і фондову біржу» від 18 червня 1991 р. № 1201-XII підлягає обов'язковому опублікуванню.

Отже, підприємство може вважати комерційною таємницею практично будь-яку інформацію про свою діяльність та свій персонал і самостійно організовувати її захист.

Усі види інформації, які можуть вважатися комерційною таємницею, можна умовно поділити на дві групи:

1) науково-технічна (технологічна) інформація;

2) ділова (комерційна) інформація.

До першої групи належать незапатентовані науково-технічні розробки, бази даних та інші комп'ютерні програми, створені підприємством, усі види «ноу-хау», технічні проекти, промислові зразки, незапатентовані товарні знаки тощо.

Ділова інформація містить:

– відомості про фінансову сторону діяльності підприємства, крім фінансових звітів (стан розрахунків з клієнтами, заборгованість, кредити та ін.);

– відомості про розмір прибутку, собівартості виробленої продукції тощо;

– плани розвитку підприємства (тактичні і стратегічні);

– плани й обсяги реалізацій продукції (плани маркетингу, дані про характер і обсяг торгових операцій, про рівні цін, наявність то варів);

– аналіз конкурентоспроможності виробленої продукції, ефективність експорту та імпорту, прогнозований час виходу на ринок;

– плани рекламної діяльності;

– списки торгових та інших клієнтів, представників, посередників, конкурентів, відомості про взаємовідносини з ними, їх фінансове положення, проведені операції, умови діючих і нових контрактів та ін.

Інформація підприємства, що становить комерційну таємницю, за важливістю може належати до чотирьох рівнів:

1. Життєво важлива – незамінна інформація, наявність якої стратегічно необхідна для функціонування підприємства. Витік цієї інформації ставить під загрозу функціонування підприємства.

2. Важлива – інформація, процес ліквідації наслідків витоку якої складний або пов'язаний з великими витратами.

3. Корисна – інформація, витік якої завдає матеріальної шкоди підприємству, однак воно може ефективно функціонувати й у разі витоку цієї інформації.

4. Неістотна – інформація, витік якої не завдає матеріального збитку підприємству і не впливає на його функціонування.

Уся ця інформація має різну цінність для підприємця, і розголошування її може призвести (або не призвести) до загроз економічній безпеці різного ступеня важкості. Тому інформацію доцільно поділяти на три групи:

а) інформація для відкритого користування будь-яким споживачем у будь-якій формі;

б) інформація обмеженого доступу – тільки для органів, що мають відповідні законодавчо встановлені права (міліція, податкова поліція, прокуратура);

в) інформація тільки для працівників (або керівників) підприємства. Інформація, що належить до другої і третьої груп, є конфіденційною і має обмеження у розповсюдженні.

4.3. Організація захисту комерційної таємниці на підприємстві

Для безпосереднього визначення переліку відомостей, що становлять комерційну таємницю, на підприємстві відповідним наказом керівника створюється спеціальна комісія, яка займається групуванням і уточненням інформації для цього переліку. Чисельність такої комісії не повинна перевищувати чотирьох-п'яти осіб.

Зазначеним наказом керівники всіх підрозділів і установ суб'єкта підприємництва зобов'язуються виокремити відомості по своїх напрямах роботи, які з їх погляду вимагають обмеження доступу до них шляхом надання їм категорії комерційної таємниці. Пропозиції підрозділів надходять до зазначеної вище комісії, яка їх обробляє, перевіряє щодо відповідності вимогам чинного законодавства, формує і узгоджує в підрозділах остаточний проект переліку таких відомостей. Зазначений перелік надається керівнику суб'єкта підприємництва, який відповідним наказом вводить його в дію. Одночасно в наказі визначаються особи, яким інформація, що складає комерційну таємницю може розкриватись в повному обсязі.

При оформленні переліку відомостей, що становлять комерційну таємницю, у своїй діяльності комісія має керуватися наступним:

– якщо підприємство має у своєму розпорядженні інформацію, яка належить до державної таємниці, її слід виділити в окрему позицію, оскільки цей вид інформації охороняється законодавством України про державну таємницю;

– в окрему позицію також слід виділити ту інформацію, яка не є комерційною таємницею згідно з Постановою № 611;

– обов'язково до комерційної таємниці мають бути віднесені різні види «ноу-хау»; різні договори також повинні вважатися комерційною таємницею, причому як сам текст договору, так і факт їх укладення; мають бути віднесені до комерційної таємниці й відомості про винаходи і рацпропозиції, які не захищені авторським або патентним правом.

Крім затвердження такого переліку на керівника підприємства покладається також обов'язок щодо встановлення порядку захисту комерційної таємниці. Серед методів такого захисту можна виділити:

– розробку положення про комерційну таємницю на підприємстві;

– розробку інструкцій щодо дотримання працівниками режиму нерозголошення комерційної таємниці;

– включення до статуту підприємства розділів, які регламентують захист комерційної таємниці;

– *встановлення кола осіб, які мають доступ до такої інформації;*

– розробку угоди про нерозголошення комерційної таємниці, що укладається з особами, які мають доступ до цієї інформації;

– встановлення *правил роботи з документами, позначеними грифом «КТ».*

Перед тим як взяти з працівників підписку про нерозголошення відомостей, що становлять комерційну таємницю, керівництву підприємства необхідно здійснити певні процедури:

– видати наказ по підприємству про встановлення комерційної таємниці;

– затвердити перелік відомостей, що становлять комерційну таємницю;

– затвердити форму зобов'язання (договору) про нерозголошення інформації, що є комерційною таємницею; інколи порядок захисту комерційної таємниці обумовлюється в трудовому контракті з працівником;

Незалежно від обраного підприємством шляху захисту комерційної таємниці працівник, приступаючи до виконання своїх обов'язків, має бути поінформований:

– про порядок і процедуру набуття матеріалами, документами та виробами статусу комерційної таємниці підприємця;

– про правила, пов'язані з доступом до інформації, що є комерційною таємницею;

– про обов'язки й обмеження, що покладаються на виконавців, допущених до відомостей конфіденційного характеру (наприклад, діловодство, облік, збереження, розмноження, обробка інформації тощо);

– про порядок прийому представників інших суб'єктів підприємницької діяльності та передачі їм інформації;

– про відповідальність за розголошення відомостей, що складають комерційну таємницю підприємства, або за порушення встановленого порядку роботи з ними.

4.4. Система захисту інформації на підприємстві

З інформаційної точки зору підприємство являє собою комплекс компонентів, пов'язаних між собою єдиною метою, структурними відносинами, технологіями інформаційного обміну. Ці компоненти: персонал, технічні засоби інформатизації, програмне забезпечення, документи можна вважати об'єктами захисту інформації.

Забезпечення інформаційної безпеки має носити системний та комплексний характер. Системність заходів інформаційної безпеки суб'єктів підприємництва має передбачати наступне:

– високий ступінь захищеності їх інформації як головну характеристику її якісного стану;

– заходами безпеки охоплюються всі інформаційні ресурси суб'єктів підприємництва;

– діяльність із забезпечення інформаційної безпеки є безперервною і плановою, на основі єдиної концепції безпеки;

– забезпечення інформаційної безпеки здійснюється у тісній єдності з поточною діяльністю суб'єктів підприємництва.

Комплексний характер системи забезпечує оптимізацію заходів та засобів, що використовуються нею задля створення необхідного балансу вимог і можливостей інформаційної безпеки. Комплексний підхід обумовлюється ще і тим, що загрози інформації суб'єктів підприємництва носять різноманітний характер, перекриття яких вимагає застосування багатьох, різних за призначенням заходів і засобів.

Система захисту інформації підприємства – це організована сукупність об'єктів і суб'єктів захисту інформації, заходів, методів, засобів та технологій, що використовуються для захисту його інформаційних ресурсів.

Основна мета створення системи захисту інформації – забезпечення надійного зберігання і ефективного використання інформації в діяльності підприємства.

Алгоритм роботи щодо організації системи захисту інформації вміщує такі дії:

– визначення вразливості інформації суб'єкта підприємництва (виявлення в інформаційній системі суб'єкта місць, використання зловмисниками яких може нанести шкоди інформаційним ресурсам і в цілому суб'єкту підприємництва);

– визначення мети, завдань та об'єктів захисту інформації;

– вибір форм, способів та засобів захисту інформації;

– формування елементів системи захисту інформації, її сил та засобів;

– створення нормативної бази суб'єкта з питань захисту інформації;

– планування функціонування системи, використання нею сил та засобів захисту інформації у відповідності до особливостей діяльності суб'єкта підприємництва;

– забезпечення взаємодії всіх елементів системи між собою та з іншими компонентами, які згідно політики інформаційної безпеки можуть бути задіяні для захисту інформації;

– забезпечення функціонування системи (матеріальне, фінансове, наукове та ін.);

– контроль стану захищеності інформації, надійності функціонування системи та ефективності заходів, що вживаються нею.

Вразливість інформації є одним із головних показників стану її захищеності. Тому визначення ступеня вразливості інформації у ході організації її захисту має досить суттєве значення.

Результати, отримані в ході визначення вразливості інформації, використовуються для встановлення складу інформації, яка підлягає безпосередньому захисту, тобто об'єктів захисту. Загальний підхід тут полягає у тому, що захисту підлягає вся інформація з обмеженим доступом і найбільш важлива частина відкритої інформації. При цьому інформація з обмеженим доступом повинна захищатись від втрати і несанкціонованого витоку, а відкрита – тільки від втрати.

Враховуючи різноманітність загроз інформації суб'єктів підприємництва та необхідність найбільш ефективного її захисту, система має виконувати відповідний **комплекс завдань:**

1. Завдання правового характеру:

– регулювання доступу до інформаційних ресурсів підприємства представників державних органів і установ;

– регулювання доступу персоналу до інформаційних ресурсів підприємства.

2. Завдання організаційного характеру:

– категоріювання інформації підприємства;

– встановлення відповідного режиму роботи підприємства;

– організація спеціального діловодства в діяльності підприємства;

– підбір персоналу для роботи з інформацією, що має обмежений доступ;

– профілактична та виховна робота з персоналом;

– здійснення заходів захисту інформації у ході зустрічей, ділових переговорів, конференцій тощо;

– планування дій щодо захисту інформації при стихійних лихах, пожежах, терористичних актах, інших негараздах.

3. Завдання інженерно-технічного характеру:

– спеціальне інженерно-технічне обладнання місць зберігання інформації;

– застосування спеціальних технічних засобів для перекриття різних видів каналів витоку інформації;

– застосування технічних засобів охорони та технічна укріпленість об'єктів.

4. Завдання криптографічного характеру:

– шифрування інформації при передачі її через незахищені засоби зв'язку;

– регламентація доступу до баз даних та електронних документів.

5. Завдання програмно-апаратного характеру:

– застосування спеціальних програмних засобів захисту комп'ютерної інформації;

– застосування антивірусних програм;

– забезпечення безперебійної роботи комп'ютерних систем при аварійних ситуаціях;

– виключення можливості перехоплення електромагнітних випромінювань і наводок;

– створення системи страхового копіювання комп'ютерної інформації.

Особливим об'єктом захисту інформації в діяльності суб'єктів підприємництва є персонал, в пам'яті якого зосереджено величезні масиви інформації, в тому числі і такої, що є цінною для суб'єктів.

У цьому сенсі працівники суб'єктів підприємництва як носії інформації характеризуються з точки зору її захисту позитивними та негативними рисами. Позитивним є те, що без згоди суб'єктів із пам'яті працівників ніяка інформація ні за яких умов не може бути вилучена, працівники можуть об'єктивно оцінювати важливість інформації, якою володіють і відповідно до цього ставитись до неї, а також ранжувати споживачів їхньої інформації, знаючи кому і яку інформацію можна довірити.

Негативним є те, що працівники можуть помилятись в щирості таких споживачів, бути не повністю компетентним у важливості інформації, якою володіють, їх дії багато в чому залежать від емоційного стану, характеру, власних потреб.

За таких умов система захисту інформації щодо об'єкту захисту такого як працівники має вживати заходи регламентування роботи працівників з інформацією, встановлювати відповідні обмеження та заборони, а також певним чином мотивувати поведінку працівників до дотримання встановленого режиму захисту інформації.

Регламентування роботи працівників з інформацією здійснюється шляхом:

– визначення осіб, яким надано право доступу до інформації повному обсязі;

– визначення осіб, яким надано право доступу до інформації суб'єкта підприємництва в частині, що їх стосується;

– встановлення порядку доступу до інформації суб'єкта підприємництва та повноважень осіб щодо її використання;

– визначення порядку та правил використання носіїв інформації в процесі діяльності суб'єкта підприємництва;

– визначення порядку та правил зберігання інформації, вироблення, обліку та пересилання електронних та паперових документів.

Мотивації у забезпеченні захисту інформації, якою володіють працівники формуються через зацікавленість працівників у виконанні ними заходів захисту. Основними методами тут виступають: формування у працівників фірмового патріотизму; матеріальна та кар'єрна вигода

дотримання заходів захисту; відповідне відношенні колективу до осіб, що порушують встановлені правила захисту інформації; зручність виконання зазначених заходів тощо.

Захист інтересів суб'єктів підприємництва у взаємовідносинах з персоналом, допущеним до їх таємниць здійснюється шляхом правового закріплення таких взаємовідносин у документах: зобов'язанні про нерозголошення інформації з обмеженим доступом; трудовому договорі (контракті); наказі про призначення на посаду; посадовій інструкції.

У захисті інформації підприємства важливе місце відводиться організації спеціального діловодства. Діловодство розуміється як система заходів по документаційному забезпеченню діяльності суб'єкта підприємництва. Основним правилом в організації діловодства і захисту інформаційних ресурсів є забезпечення розмежування потоків відкритої інформації і інформації з обмеженим доступом. За таких *умов в діяльності* суб'єктів підприємництва має бути організовано службове діловодство (забезпечення документообігу відкритої інформації) і спеціальне діловодство, яке забезпечує документообіг інформаційних матеріалів таємного та конфіденційного характеру.

Важливу роль у забезпеченні ефективного функціонування системи захисту інформації в діяльності суб'єктів підприємництва відіграє правильне управління такою системою, яка має здійснюватись централізовано на рівні головної установи певного суб'єкта. Насамперед воно передбачає вироблення правил, норм, стандартів захисту інформації, їх деталізації, по силах і засобах, залучених до захисту інформації.

З метою забезпечення цілеспрямованого і організованого впливу на функціонування системи має здійснюватись конкретизація та періодичне уточнення завдань всім підрозділам, установам з питань захисту інформації. Конкретизація завдань має випливати із аналізу ситуації, що складається в той чи інший час. Важливим в управлінні є здійснення контролю в системі захисту інформації, який передбачає проведення різного роду перевірок, періодичне отримання звітів про результати виконання заходів захисту, аналіз показників функціонування системи та оцінку ефективності її в цілому.

ЗМІСТОВИЙ МОДУЛЬ ІІ.
ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА ТА УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ

ТЕМА 5
ПРАВОВІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

5.1. Правові умови забезпечення інформаційної безпеки на підприємстві

5.2. Правове регулювання відносин у сфері захисту інформації з обмеженим доступом

5.3. Право інтелектуальної власності на комерційну таємницю

5.4. Відповідальність за незаконні дії щодо комерційної таємниці на підприємстві

5.1. Правові умови забезпечення інформаційної безпеки на підприємстві

Забезпечення інформаційної безпеки підприємницької діяльності здійснюються під впливом різноманітних умов, серед яких провідне місце займають правові умови.

Правові умови утворюються такими джерелами правових норм: Конституцією України, законодавчими актами, підзаконними актами, нормативно-правовими актами підприємств.

Правові умови визначають можливість організації інформаційної безпеки на підприємстві. За допомогою зазначених актів здійснюється:

– регулювання інформаційних відносин та застосування заходів інформаційної безпеки;

– визначається правомірність тих чи інших дій щодо інформації;

– формуються підстави для відповідальності за дії в інформаційному просторі.

Правові норми забезпечують захист підприємств від неправомірного посягання на їх права, інтелектуальну власність, інформацію, що може мати місце у процесі їх діяльності.

Право на інформацію передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів.

Конституцією України гарантується право судового захисту щодо спростування недостовірної інформації, право вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням та поширенням недостовірної інформації.

Основний закон забороняє збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків визначених законом (ст. 32 Конституції України). До конфіденційної інформації про особу належать дані про національність особи, освіту, сімейний стан, релігійні переконання, стан здоров’я, а також адресу, дату і місце

народження. Тобто Конституція України встановлює загальні умови поведінки суб'єктів господарювання і громадян в інформаційному просторі.

Важливим моментом для забезпечення правової поведінки в інформаційному просторі і правомірних інформаційних відносин є регулювання доступу до інформації (відкрита інформація та з обмеженим доступом). Ці питання регулюються положеннями Закону України «Про інформацію».

Будь-яка інформація є відкритою крім тієї, що віднесена законом до такої, що має обмежений доступ.

Конфіденційна інформація – інформація, доступ до якої обмежено фізичною чи юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов.

До суб'єктів владних повноважень законодавець відносить – органи державної влади, місцевого самоврядування, інших суб'єктів, що здійснюють владні управлінські функції відповідно до законодавства, в т.ч. і делеговані повноваження.

Важливим є з'ясування особи, яка має право обмежувати доступ та надавати інформації категорію конфіденційної. Очевидно, що це може бути сам власник такої інформації, або особа, яка отримує право розпоряджатись даною інформацією. У останньому випадку законодавець визначає перелік розпорядників інформації, види інформації, якими вони можуть розпоряджатись, їх обов'язки та функції (Закон України «Про доступ до публічної інформації» ст. ст. 13-18).

Таємною є інформація, доступ до якої обмежується відповідно до вимог ст.6 Закону України «Про доступ до публічної інформації» і розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить відомості, що складають державну, професійну, банківську таємницю, таємницю досудового розслідування та інші передбачені законом види таємниць.

До службової інформації належить така, що міститься в документах суб'єктів владних повноважень, а також зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Доступ до таємної інформації визначається відповідно до чинного законодавства установами, органами, які володіють такою інформацією. Доступ до службової інформації визначається відповідно до Закону України «Про доступ до публічної інформації» в порядку передбаченому внутрішніми документами суб'єкта владних повноважень.

Відносини у сфері доступу до публічної інформації регулюються Законом України «Про доступ до публічної інформації». Зокрема, закон дає визначення поняття «публічна інформація» згідно з яким це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка

знаходиться у володінні таких суб'єктів, інших розпорядників, крім випадків встановлених законом.

Відповідно до зазначеного вище закону, доступ до публічної інформації здійснюється шляхом її оприлюднення у встановленому порядку та шляхом подання запитів до розпорядників інформації. Інформація надається безкоштовно.

Суб'єктами відносин у сфері доступу до публічної інформації є запитувачі інформації, розпорядники інформації, їх структурні підрозділи або відповідальні особи з питань виконання запитів.

Окремо регулюється система відносин щодо доступу до інформації про особу. Тут маємо брати за основу положення Закону України «Про захист персональних даних», Закону України «Про доступ до публічної інформації», Закону України «Про інформацію». Зокрема передбачається, що збирання, зберігання, використання та поширення інформації про особу не можливе без згоди самої особи, крім випадків передбачених законом. Обсяг такої інформації має бути максимально обмеженим і використовуватись лише з метою та у спосіб, визначений законом.

Суб'єктами відносин у сфері доступу до інформації про особу виступають суб'єкти персональних даних, володільці та розпорядники баз персональних даних, треті особи (особи, яким володільцями чи розпорядниками баз персональних даних здійснюється передача персональних даних відповідно до закону), уповноважений ВРУ з прав людини, інші державні органи, органи місцевого самоврядування, до повноважень яких належить здійснення захисту персональних даних.

Поширення персональних даних здійснюється лише за згодою особи. Без згоди – у випадках визначених законом і лише в інтересах національної безпеки, економічного добробуту та прав людини. Порядок доступу до персональних даних та відносини суб'єктів з цих питань регулюються положеннями ст.ст. 16–19 Закону України «Про захист персональних даних».

Питання правового регулювання доступу до персональних даних нормами міжнародного права, забезпечуються:

– положеннями Конвенції Ради Європи «Про захист фізичних осіб при автоматизованій обробці персональних даних» від 28.01.1981р. зі змінами внесеними у 1999р.;

– додаткового протоколу до Конвенції «Про захист фізичних осіб при автоматизованій обробці персональних даних щодо органів нагляду і трансграничних потоків даних» від 08.11.2001 року;

– Директивою Ради Європейського Союзу «Про захист фізичних осіб при автоматизованій обробці персональних даних і про вільний обіг таких даних» (1995р.);

– Директивою «Про обробку персональних даних і захист прав фізичних осіб у телекомунікаційному секторі» (1997р.).

5.2. Правове регулювання відносин у сфері захисту інформації з обмеженим доступом

Важливе значення, з точки зору інформаційної безпеки, має правове регулювання відносин у сфері захисту інформації з обмеженим доступом. Для підприємницької діяльності важливими питаннями є захист комерційної та банківської таємниці, а також комерційної інформації.

Правову основу комерційної таємниці складають положення Господарського кодексу України, Цивільного кодексу України, Кримінального кодексу України, Кодексу України про адміністративні правопорушення, Законів України «Про захист від недобросовісної конкуренції», «Про інформацію», інших правових актів.

Зокрема, сутність комерційної таємниці як виду інформації з обмеженим доступом, подається у Цивільному кодексі України.

Так, **комерційною таємницею** є інформація, яка є секретною в тому розумінні, що вона в цілому чи певній формі та сукупності її складових є невід'ємною та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить і у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію.

За змістом комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці.

Такий вид таємниці як комерційна стосується лише суб'єктів господарювання: юридичних осіб та фізичних осіб зареєстрованих як суб'єкти підприємницької діяльності. Право власності на такий вид інформації вони отримують через створення її власними силами та засобами або іншими особами на договірних засадах з суб'єктами господарювання за їх кошти і на їх користь, придбанням такої інформації у інших осіб.

Окремо регулюється порядок захисту комерційної таємниці суб'єктів господарювання у їх конкурентних відносинах. Так, відповідно до гл. 4 Закону України «Про захист від недобросовісної конкуренції»:

– неправомірним визнається збирання протиправним способом відомостей, що становлять комерційну таємницю за умов коли це завдало чи могло завдати шкоди суб'єкту господарювання;

– неправомірним визнається впровадження у виробництво або врахування під час планування чи здійснення господарської діяльності без дозволу уповноваженої на те особи (неправомірне використання) відомостей, що становлять комерційну таємницю;

– неправомірним визнається розголошення комерційної таємниці, тобто ознайомлення іншої особи без дозволу особи, уповноваженої на те, з відомостями, що відповідно до законодавства України становлять комерційну таємницю, особою, якій ці відомості були довірені або стали відомі у зв'язку з

виконанням відповідних обов'язків, якщо це завдало чи могло завдати шкоди суб'єкту господарювання;

– неправомірним вважається схилення до розголошення комерційної таємниці, тобто спонукання особи, якій були довірені у встановленому порядку або стали відомі у зв'язку з виконанням відповідних обов'язків відомості, що відповідно до законодавства України становлять комерційну таємницю, до розкриття цих відомостей, якщо це завдало чи могло завдати шкоди суб'єкту господарювання.

Такі дії суперечать нормам чинного законодавства і переслідуються у кримінальному, адміністративному чи цивільному (відшкодування шкоди) порядку.

Певну специфіку мають інформаційні відносини, предметом яких є **банківська таємниця.**

Згідно ст. 60 Закону України «Про банки і банківську діяльність» **банківською таємницею** є інформація щодо діяльності та фінансового стану клієнтів банку, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним чи третіми особами при наданні послуг банку.

Тобто, банківська таємниця виникає тоді коли суб'єкти господарювання (підприємництва) стають клієнтами банків. Останні вважаються такими у разі отримання послуг банків. Враховуючи ж, що вказані суб'єкти здійснюючи свою фінансово-господарську діяльність обов'язково вдаються до послуг банків, виникнення в них банківської таємниці є закономірним фактом. В той же час слід зазначити, що статус банківської таємниці діє навіть тоді, коли суб'єкт (клієнт) припиняє відносини з банком. Інформація, що надана банку залишається в банку і закон не передбачає, що втрата відносин клієнта з банком припиняє статус банківської таємниці.

Зміст банківської таємниці конкретизовано у зазначеному законі і він є остаточним аж до поки в закон в установленому порядку не буде внесено відповідних змін. Зокрема вказується, що до складу банківської таємниці віднесено:

– відомості про банківські рахунки клієнтів, в т. ч. кореспондентські рахунки банків у НБУ;

– операції, які були проведені на користь чи за дорученням клієнтів, здійснені ними угоди;

– фінансово-економічний стан клієнтів;

– відомості про системи охорони банку і клієнтів;

– інформація про організаційно-правову структуру юридичної особи клієнтів, їх керівників, напрями діяльності;

– відомості стосовно комерційної діяльності клієнтів чи їх комерційної таємниці, будь-якого проекту, винаходів, зразків продукції та інша комерційна інформація;

– інформація щодо звітності по окремому банку за винятком тієї, що підлягає опублікуванню (ст. 70) Закону України «Про банки і банківську діяльність»;

– коди, що використовуються банками для захисту інформації.

Тут слід додати, що у зв'язку з появою законодавства про захист персональних даних, НБУ вніс певні доповнення до змісту банківської таємниці. Відповідно до постанови Правління НБУ від 11.07.2012р. №292 банківською таємницею є відомості або сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, що стали відомі банку під час обслуговування фізичної особи та взаємовідносин з нею та взаємовідносин з нею чи третіми особами при наданні послуг банку.

Тобто, за своєю суттю і змістом банківська таємниця є єдиною для всіх банків і їх клієнтів, на відміну від комерційної таємниці.

Враховуючи особливий статус та значний обсяг електронної інформації в діяльності суб'єктів підприємництва законодавець передбачив відповідні правові умови відносин у сфері такої інформації. Основним правовим документом тут є Закон України «Про захист інформації в інформаційно-телекомунікаційних системах».

Згідно закону об'єктами захисту виступають:

– інформація, що використовується в інформаційно-телекомунікаційних системах;

– програмне забезпечення, яке використовується для обробки інформації.

Суб'єктами відносин, пов'язаних із захистом інформації в інформаційно-телекомунікаційних системах є:

– володільці інформації;

– власники систем;

– користувачі;

– уповноважений орган виконавчої влади з питань організації спецзв'язку та захисту інформації і підпорядковані йому регіональні органи

Взаємовідносини суб'єктів здійснюється на договірних засадах.

Порядок доступу до інформації, що оброблюється в системі, перелік користувачів та їх повноваження визначає власник інформації. У випадках коли в системах оброблюється інформація з обмеженим доступом, доступ до неї визначається законодавством. Положеннями закону врегульовано відносини поміж власниками інформації і власниками інформаційно-телекомунікаційних систем, між власниками різних систем, власниками систем і користувачами. Організація захисту інформації, що оброблюється у системах покладається на власників систем. За порушення порядку і правил захисту інформації, що оброблюється в інформаційно-телекомунікаційних системах може наступати адміністративна та кримінальна відповідальність.

Документообіг в електронному інформаційному просторі на сьогоднішній час є одним із елементів документування підприємницької діяльності. Безумовно, що він має бути в правовому плані врегульованим і захищеним. Це питання регулюється двома законодавчими актами: Закони України «Про електронні документи та електронний документообіг» і «Про електронний цифровий підпис», а також Положеннями «Про технічний захист інформації в Україні» і «Про порядок здійснення криптографічного захисту інформації в Україні».

Вказані вище Положення визначають порядок технічного захисту інформації та виконання криптографічного захисту інформації з обмеженим доступом.

Організовуючи забезпечення інформаційної безпеки суб'єктів підприємництва у стосунках з представниками засобів масової інформації необхідно досить грамотно орієнтуватись у законодавстві та правових актах, що регулюють діяльність суб'єктів масової інформації.

Зокрема доцільним буде ознайомлення з положеннями наступних правових актів:

– Закону України «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації»;

– Закону України «Про інформацію»;

– Закону України «Про друковані засоби масової інформації (пресу) в Україні»;

– Закону України «Про телебачення і радіомовлення»;

– Закону України «Про інформаційні агентства»;

– Закону України «Про авторське право і суміжні права»;

– Закону України «Про державну підтримку засобів масової інформації та соціальний захист журналістів»;

– Закону України «Про захист суспільної моралі».

Крім того, не зайвим буде ознайомитись з Кодексом професійної етики українського журналіста.

Враховуючи, що діяльність з забезпечення інформаційної безпеки суб'єктів підприємництва зазвичай передбачає взаємовідносини з правоохоронними та судовими органами, органами контролю та нагляду, які керуються спеціальними законодавчими актами, що регулюють їх діяльність, доцільним також буде ознайомлення з правами таких органів в інформаційній сфері:

– Закону України «Про прокуратуру»;

– Закону України «Про Національну поліцію»;

– Закону України «Про службу безпеки України»;

– Закону України «Про оперативно розшукову діяльність»;

– Закону України «Про організаційні основи боротьби з організованою злочинністю»;

– Закону України «Про судоустрій та статус судів»;

– Закону України «Про адвокатуру та адвокатську діяльність»;

– Закону України «Про Національний банк України»;

– Податкового кодексу України та іншими положеннями правових актів, що регулюють діяльність зазначених органів.

Питання правового регулювання інформаційної безпеки суб'єктів підприємництва не буде повним без нормативно-правових документів самих суб'єктів. Саме такі нормативно-правові документи, базуючись на положеннях законодавчих та підзаконних актів утворюють правові підстави та регулюють діяльність суб'єктів щодо встановлення відповідного інформаційного режиму

їх інформаційних відносин з іншими суб'єктами, контрагентами, клієнтами, кредиторами і мають певне значення для взаємостосунків з державними органами. Якраз в таких документах обґрунтовується поведінка суб'єктів підприємництва в їх інформаційному просторі за різних умов.

На жаль на сьогодні, як і взагалі у сфері інформаційної безпеки суб'єктів підприємництва, так і в питаннях правового її регулювання нормативно-правовими документами самих суб'єктів стійкої позиції немає. Беручи до уваги мету, завдання та зміст інформаційної безпеки суб'єктів підприємництва, структуру процесу її організації та напрацьований досвід, можна рекомендувати наступний перелік таких нормативно-правових документів:

– Положення про комерційну таємницю та правила її зберігання на підприємстві;

– Положення про конфіденційну інформацію підприємства;

– Інструкція про порядок підготовки, обліку, зберігання та знищення документів, справ, видань і матеріалів, що містять комерційну таємницю та конфіденційну інформацію підприємства ;

– Положення про захист електронної інформації та електронних документів на підприємстві;

– Інструкція про порядок виконання документів, що надходять до підприємства від правоохоронних органів, судів та інших державних установ;

– Положення про архів і архівну діяльність підприємства;

– Інструкція про проведення службових розслідувань на підприємстві;

– Положення про інформаційно-аналітичну роботу на підприємстві;

– Інструкція з службового діловодства;

– Інструкція з спеціального діловодства;

– Правила використання, поширення та зберігання інформації підприємства у процесі його діяльності;

– Методики розробки інформаційних документів підприємства та надання інформаційних послуг;

– Пам'ятки працівникам підприємства щодо збереження інформації з обмеженим доступом тощо.

Незважаючи на значний перелік документів, всі вони утворюють правове поле суб'єкта підприємництва у сфері забезпечення його інформаційної безпеки, обґрунтовують поведінку суб'єкта у інформаційному середовищі.

5.3. Право інтелектуальної власності на комерційну таємницю

Створення інформації, що становить комерційну таємницю іншими особами на користь суб'єктів господарювання стосується зазвичай продуктів інтелектуальної власності. Комерційною таємницею у таких випадках захищаються інформаційні характеристики зазначених продуктів. Право власності включає право володіння, право використання і право розпорядження чи поширення.

Враховуючи, що суб'єкти господарювання є власниками своєї комерційної таємниці, вони ж самі визначають умови та способи їх захисту, доступу до неї, в т. ч. і у будь-яких взаємовідносинах з іншими суб'єктами.

Згідно з положеннями Цивільного кодексу України (ст. 506) право розкриття комерційної таємниці належить особі, яка володіє майновими правами інтелектуальної власності на комерційну таємницю. Тобто, підстави, умови, способи захисту відомостей, що становлять комерційну таємницю у різних суб'єктів господарювання можуть бути різними, організуються кожним із них, виходячи з особливостей їх діяльності, інформаційних потреб та можливостей. Інформаційні відносини суб'єктів господарювання щодо комерційної таємниці, як правило, будуються на договірних засадах, з врахуванням нормативних документів суб'єктів у сфері їх інформаційної безпеки.

Право інтелектуальної власності на комерційну таємницю визначається Цивільним кодексом України.

Комерційна таємниця як об'єкт інтелектуальної власності має **свої особливості.**

По-перше, вона відрізняється найбільшою універсальністю, оскільки комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком тих, які відповідно до закону не можуть бути віднесені до комерційної таємниці.

По-друге, для виникнення прав на комерційну таємницю не вимагається виконання будь-яких формальностей, офіційного визнання її охороноздатності та державної реєстрації.

По-третє, оскільки в її основі лежить фактична монополія певної особи на деякі знання, то строк чинності права інтелектуальної власності на комерційну таємницю чітко не визначений і обмежується строком існування сукупності зазначених ознак комерційної таємниці.

Ознаками комерційної таємниці є:

– інформація, що становить комерційну таємницю має комерційну цінність;

– інформація, що становить комерційну таємницю, не відома іншим особам та відсутній вільний доступ до неї на законних підставах;

– вжито заходів для охорони конфіденційної інформації.

Ці ознаки комерційної таємниці є істотними, необхідними та невіддільними.

Майновими правами інтелектуальної власності на комерційну таємницю є (ст. 506 Цивільного кодексу):

– право на використання комерційної таємниці;

– виключне право дозволяти використання комерційної таємниці;

– виключне право перешкоджати неправомірному розголошенню, збиранню або використанню комерційної таємниці;

– інші майнові права інтелектуальної власності, встановлені законом.

Майнові права інтелектуальної власності на комерційну таємницю належать особі, яка правомірно визначила інформацію комерційною, якщо інше не встановлено договором.

Саме ця особа може розпорядитися належним їй об'єктом, зокрема, шляхом розкриття відомостей невизначеному колу осіб.

Суб’єкт права інтелектуальної власності вправі в будь-який спосіб, не порушуючи прав інших осіб, використовувати комерційну таємницю. Він може передати іншій особі для використання останньою цієї інформації в її діяльності, зберігаючи чи не зберігаючи при цьому права на використання комерційної інформації у власній діяльності.

Особа, що порушила право інтелектуальної власності на комерційну таємницю, несе відповідальність, яка встановлена законом або договором. Зазвичай така відповідальність полягає у відшкодуванні шкоди. Якщо доступ до комерційної таємниці особа отримала на підставі договору, можливе встановлення договором неустойки за порушення права інтелектуальної власності на комерційну таємницю.

Суб’єктами, що несуть відповідальність перед власником комерційної таємниці, можуть бути юридичні особи, фізичні особи (якщо за них відповідно до законодавства не несе відповідальність юридична особа), в тому числі працівники юридичної чи фізичної особи — власника комерційної таємниці.

Інформація, що становить комерційну таємницю, має бути предметом адекватних існуючим обставинам заходів щодо збереження її конфіденційності, вжитих особою, яка законно контролює цю інформацію.

Строк чинності права інтелектуальної власності на комерційну таємницю визначається ст. 508 ЦК.

Строк чинності права інтелектуальної власності на комерційну таємницю обмежується строком існування сукупності ознак комерційної таємниці, встановлених частиною першою статті 505 Цивільного кодексу.

5.4. Правова відповідальність за незаконні дії щодо комерційної таємниці на підприємстві

За посягання на комерційну таємницю законодавство України передбачає дисциплінарну, кримінальну, адміністративну та цивільну відповідальність.

Тут слід виділити дві основні групи суб’єктів посягань на таку інформацію. Особи, що незаконно заволоділи інформацією та особи, що правомірно отримали таку інформацію, але порушили зобов’язання щодо збереження її в таємниці (працівники, контрагенти, партнери, клієнти, державні службовці).

Неправомірне збирання, розголошення та використання комерційної таємниці є видом недобросовісної конкуренції, який може становити досить серйозну загрозу економічній безпеці підприємства.

Адміністративна відповідальність. Ст.ст. 16–19 Закону України «Про захист від недобросовісної конкуренції» (07.06.1996 р. №236/96-ВР) визначено дії, які є видами недобросовісної конкуренції, а саме: неправомірне збирання комерційної таємниці (ст. 16), розголошення комерційної таємниці (ст. 17), схилення до розголошення комерційної таємниці (ст. 18), неправомірне збирання комерційної таємниці (ст. 19).

Вчинення вищезазначених дій, тягне за собою відповідальність, передбачену вищезазначеним законом.

За такі дії передбачено накладання штрафу Антимонопольним комітетом України, його територіальними відділеннями в розмірі до п’яти відсотків виручки від реалізації товарів, виконання робіт, надання послуг господарюючого суб’єкта за останній звітний рік, що передував року, в якому накладається штраф. Слід зазначити, що штраф накладається на юридичних осіб (ст. 21 Закону № 236).

У разі якщо обчислення виручки господарюючого суб’єкта неможливе або виручки немає, штрафи, зазначені в частині першій ст. 21, накладаються в розмірі до десяти тисяч неоподатковуваних мінімумів доходів громадян (170 тис. грн.).

Збитки, заподіяні внаслідок вчинення дій, визначених згаданим вище Законом як недобросовісна конкуренція, підлягають відшкодуванню за позовами зацікавлених осіб у порядку, визначеному цивільним законодавством України (ст. 24 Закону № 236).

Крім того, частиною третьою статті 164-3 Кодексу України про адміністративні правопорушення передбачено адміністративну відповідальність за отримання, використання, розголошення комерційної таємниці, а також конфіденційної інформації з метою заподіяння шкоди діловій репутації або майну іншого підприємця. За такі дії на правопорушника накладається штраф у розмірі від дев’яти до вісімнадцяти НМДГ (від 153 грн. до 306 грн.). Нести адміністративну відповідальність, згідно із згаданою статтею, фізична особа може лише в тому випадку, коли вона вчинила дії, що свідчать про безпосереднє отримання, використання чи розголошення нею комерційної таємниці.

Щодо **цивільно-правової відповідальності** законодавство не встановлює спеціальних цивільних засобів охорони комерційної таємниці. Захист прав на комерційну таємницю можливий судом шляхом:

– визнання прав на комерційну таємницю;

– припинення дій, що порушують право на комерційну таємницю;

– компенсації моральної шкоди;

– стягнення з особи, яка порушила право, завданих збитків, включаючи неодержані доходи.

Крім того, у разі порушення комерційної таємниці можливим є застосування судом *спеціальних засобів захисту:*

– застосування негайних заходів щодо запобігання порушення прав на комерційну таємницю;

– вилучення товарів, виготовлених або введених у цивільний оборот з порушенням прав на комерційну таємницю;

– вилучення матеріалів та знарядь, які використовувалися переважно для виготовлення товарів з порушенням прав на комерційну таємницю;

– опублікування в засобах масової інформації відомостей про порушення права інтелектуальної власності на комерційну таємницю тощо.

Відповідальність в межах трудових відносин. За порушення режиму комерційної таємниці до працівника може застосовуватися матеріальна та

дисциплінарна відповідальність. Дисциплінарна відповідальність передбачає застосування таких санкцій, як догана та звільнення.

Підставою застосування до працівника дисциплінарних заходів можливо за умови підпису працівником зобов'язання про не розголошення комерційної таємниці. Розмір штрафу обумовлюється в зобов'язанні і оформляється наказом підприємства.

Працівники несуть матеріальну відповідальність перед роботодавцем за шкоду, заподіяну розголошенням комерційної таємниці відповідно до ст. 132 КЗпП (якщо працівник припустився розголошення комерційної таємниці при виконанні трудових обов'язків) або відповідно до п. 7 ст. 134 КЗпП (якщо розголошення комерційної таємниці допущене не при виконанні трудових обов'язків, хоч би комерційна таємниця і стала відома працівникові при виконанні трудових обов'язків). Не виключається повна матеріальна відповідальність працівників за шкоду, заподіяну розголошенням комерційної таємниці, на підставі п. 3 ст. 134 КЗпП, якщо дії працівника кваліфікуються як злочин, передбачений ст. 323 КК (розголошення комерційної таємниці, що завдало істотної шкоди суб'єкту господарської діяльності).

Кримінальна відповідальність. Кримінальним кодексом України (ККУ) за незаконне збирання з метою використання (комерційне шпигунство) або використання відомостей, що становлять комерційну таємницю (ст. 231 ККУ), та за розголошення комерційної таємниці (ст. 232 ККУ) передбачено кримінальну відповідальність.

Так, статтею 231 ККУ умисні дії, спрямовані на отримання відомостей, що становлять комерційну або банківську таємницю, з метою розголошення чи іншого використання цих відомостей, а також незаконне використання таких відомостей, якщо це спричинило істотну шкоду суб'єкту господарської діяльності, – караються штрафом від трьох тисяч до восьми тисяч НМДГ (від 51 тис. грн. до 136 тис. грн.).

Умисне розголошення комерційної або банківської таємниці без згоди її власника особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, якщо воно вчинене з корисливих чи інших особистих мотивів і завдало істотної шкоди суб'єкту господарської діяльності, – карається штрафом від однієї тисячі до трьох тисяч НМДГ (від 17 тис. грн. до 51 тис. грн.) з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років (ст. 232 ККУ).

Слід звернути увагу, що за статтею 232 ККУ відповідальність може нести лише обмежене коло осіб – суб'єкти, яким такі відомості стали відомі у зв'язку з їхньою професійною чи службовою діяльністю, і які, згідно з чинним законодавством, повинні їх зберігати. До таких суб'єктів можуть відноситися працівники органів державної податкової служби, банків, правоохоронних органів, особи, яким комерційну таємницю було довірено її власником, та інші суб'єкти, які, згідно з чинним законодавством, мають право на ознайомлення з відомостями, що становлять комерційну таємницю, або мають доступ до таких відомостей по службі.

ТЕМА 6
ІНФОРМАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ПІДПРИЄМСТВА

6.1. Інформаційний ресурс підприємства та його характеристика

6.2. Інформаційно-аналітична робота в діяльності підприємства

6.3. Спеціальні інформаційні операції та комерційна розвідка в діяльності підприємства.

6.1. Інформаційний ресурс підприємства та його характеристика

Інформаційний ресурс – сукупність інформації, яка знаходиться у власності чи розпорядженні підприємства і використовується ним для забезпечення діяльності.

Структуру інформаційного ресурсу з точки зору його змісту складає:

– правова інформація (нормативно-правові документи суб'єктів підприємництва, інші правові документи та матеріали);

– комерційна інформація (характеристика ринку та його суб'єктів, умови комерційної діяльності);

– ділова інформація (ділові зв'язки, партнери, взаємовідносини з ними та інша інформація, яка може бути використана в ділових стосунках);

– інформація про персонал (відомості, що містяться в особових справах працівників);

– інформація про ринки (аналітичні характеристики ринків, сфер економіки, в яких працює та планує працювати суб'єкт підприємництва);

– інформація про сферу діяльності (технології виробництва, методи забезпечення діяльності суб'єкта підприємництва, плани розвитку);

– інші види інформації (статистична, про клієнтів, наукова, про забезпечення безпеки тощо).

Таким чином, інформаційні ресурси, як сукупність інформації мають певні особливості щодо їх існування. На відміну від інших видів ресурсів, які існують в певній матеріальній формі, інформаційні ресурси представлені трьома категоріями: документами на паперових і електронних носіях, зразками продукції та інтелектом (знаннями) працівників суб'єктів підприємництва.

Важливою особливістю інформаційних ресурсів є їх багатофункціональність, вони можуть нести освітню, аналітичну, комерційну, інформуючу, маскуючу функції та функцію впливу. Така багатофункціональність інформаційних ресурсів обумовлює різнонаправлене їх використання. Зокрема, інформаційні ресурси суб'єктів підприємництва можуть використовуватись для:

– формування знань працівників підприємства, необхідних для

забезпечення професійної діяльності;

– створення нормативно-правових документів підприємства, що регулюють окремі види його діяльності та поведінку на ринку;

– формування управлінських та виробничих рішень;

– розробки нових продуктів та послуг;

– формування іміджу підприємства на ринку, забезпечення інформаційного впливу в його інформаційному середовищі;

– проведення наукових та інших досліджень, необхідних для забезпечення діяльності підприємства;

– забезпечення безпеки діяльності підприємства, ефективного проведення фінансових, комерційних, господарських та інших операцій;

– проведення інформаційно-аналітичних досліджень клієнтів, партнерів, контрагентів;

– формування перспектив розвитку підприємства.

Інформаційний ресурс є результатом роботи підприємства по інформаційному забезпеченню його діяльності. В свою чергу структуру інформаційного забезпечення складають такі види інформаційної діяльності як маркетингові дослідження, інформаційно-аналітична робота і комерційна розвідка.

Інформаційне забезпечення має відповідати наступним вимогам:

– законності – здійснюватись в межах чинного законодавства;

– безперервності – інформаційні ресурси для забезпечення їх високої якості мають постійно оновлюватись;

– активності – сили, задіяні в інформаційному забезпеченні повинні постійно прагнути до отримання інформації;

– високої технічної оснащеності – інформаційна робота повинна спиратись на сучасні комп'ютерні засоби та технології збору і обробки інформації;

– компетентності – особи, які виконують завдання інформаційного забезпечення мають бути професіоналами у своїй галузі, здатними на високому професійному рівні виконувати свої обов'язки.

Водночас організація інформаційного забезпечення, незважаючи на єдину мету здійснюється окремо по кожному з видів забезпечення: маркетингових досліджень, інформаційно-аналітичної роботи і комерційної розвідки.

Важливу роль інформаційний ресурс займає у виробленні інформаційних продуктів. Сучасні суб'єкти підприємництва здійснюють свою діяльність не лише на економічних ринках, а і ще в інформаційному середовищі. Тому інформаційні продукти, то не тільки товар, а під ними можна розуміти різного роду інформаційні та інтелектуальні матеріали, що супроводжують та забезпечують економічну діяльність суб'єктів підприємництва. Тобто, інформаційні продукти притаманні практично всім суб'єктам, які здійснюють свою діяльність на будь-якому ринку. **Інформаційними продуктами** можуть виступати технології виробництва, комерційної діяльності та взаємовідносин, результати маркетингових, соціологічних та інших досліджень, пропозиції,

проекти, аналітичні матеріали. Більш того, інформаційні продукти як інформаційні характеристики суб'єктів підприємництва чи їх діяльності можуть носити віртуальний характер, поширюючись у інформаційному просторі досить динамічно.

За своїм призначенням інформаційний ресурс суб'єктів підприємництва може мати наступну структуру:

– пізнавальний;
– виробничий;
– організаційний;
– спеціальний;
– допоміжний.

Пізнавальну частину ресурсу складає інформація, яка характеризує підприємство як комерційну організацію. Дає уявлення про можливості та результати (показники) його діяльності, продукцію, послуги, роботи; інформацію для внутрішнього користування про технології, проекти, партнерів, клієнтів, контрагентів, особливості поведінки на ринку, взаємовідносини з іншими суб'єктами; інформацію про персонал, перспективні розробки, шляхи розвитку, характеристики окремих суб'єктів, подій; ситуації.

Інформація щодо виробництва включає дані про технології, які використовуються у ході вироблення товарів, характеризують правила, умови, порядок надання послуг, виконання робіт, підходи до формування їх вартості, фінансову діяльність підприємства, іншу виробничу інформацію призначену для внутрішнього використання.

Організаційна інформація характеризує нормативно-правову складову діяльності підприємства, зміст договорів, протоколів перемовин, рішень щодо організації діяльності суб'єкта, взаємовідносин з іншими суб'єктами, сюди ж слід віднести інформацію про управління його діяльністю.

Спеціальна інформація складає дані про безпеку підприємства, його конфіденційні зв'язки, відомості з досьє осіб щодо яких має зацікавленість підприємство, зміст картотек, інтегрованих баз даних.

Допоміжна інформація – матеріали, що будь-яким чином характеризують сферу діяльності та взаємовідносин підприємства, яка отримується з локального та глобального інформаційного середовища.

Інформаційний ресурс є джерелом інформації не лише безпосередньо для самих суб'єктів підприємництва, а і для зовнішніх користувачів. Насамперед, це можуть бути кредитори, інвестори, партнери, державні органи інші суб'єкти. Тобто, інформаційний ресурс є досить структурованим за різним призначенням і доступом до інформації. Утворення такого ресурсу вимагає значної роботи. І тому не дивно, що значна частина суб'єктів підприємництва формуванню якісного, структурованого за різними ознаками інформаційного ресурсу не придає суттєвої уваги, залишаючись у сучасному інформаційному просторі недостатньо інформаційно озброєними.

6.2. Інформаційно-аналітична робота в діяльності підприємства

Інформаційно-аналітична робота (ІАР) – діяльність, пов’язана зі збором і обробкою відкритої інформації, формуванням відповідних інформаційних документів та наданням їх керівництву підприємства.

Кінцевим етапом ІАР є інформування керівництва підприємства. Структуру ІАР подано на рис. 6.1.

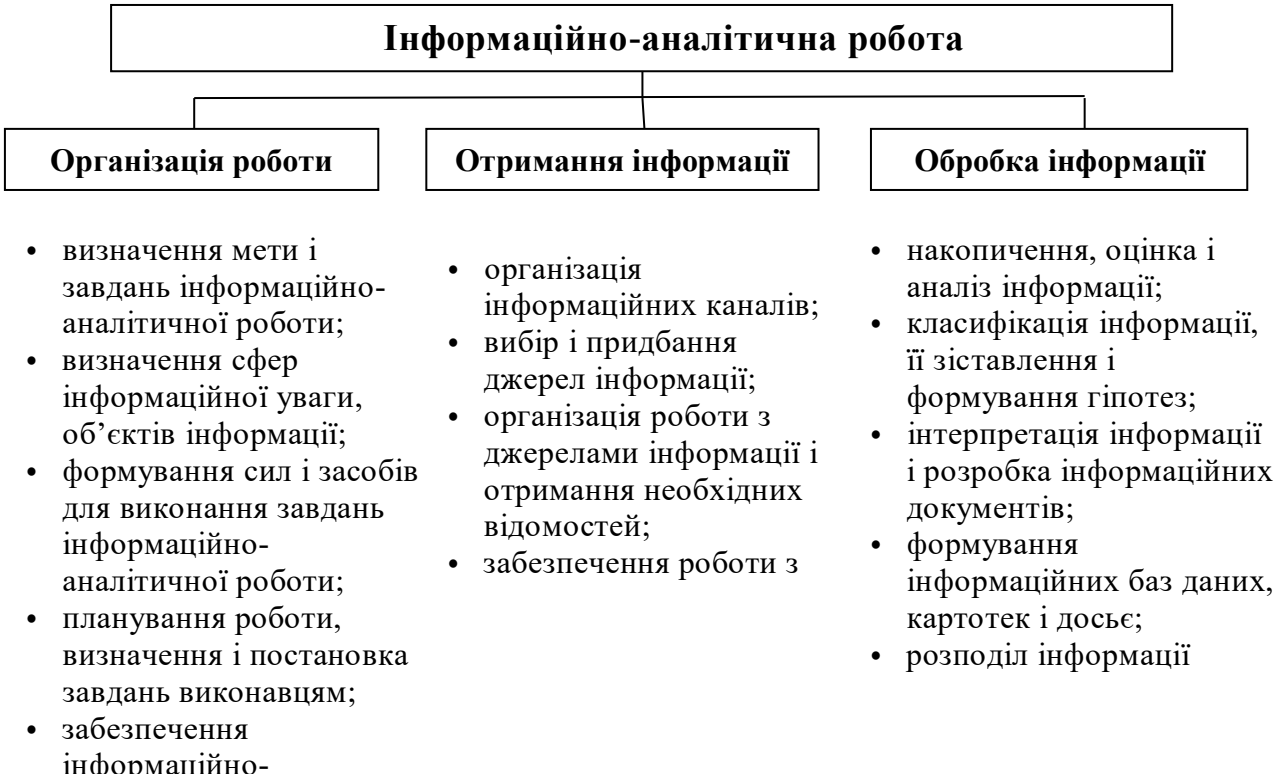

Рис. 6.1. Структура інформаційно-аналітичної роботи підприємства

Основним в організації ІАР є визначення сфер інформаційної уваги, об'єктів і джерел інформації, так як це дозволяє більш конкретизувати і спрямувати дану роботу, концентрувати зусилля суб'єктів підприємництва на найбільш важливих її напрямках. Справа в тому, що інформаційне середовище підприємницької діяльності є досить глобальним, неоднорідним, обсяги інформації в ньому є такими, що не дають можливості без ефективної організаційної роботи здійснювати інформаційне забезпечення суб'єктів підприємництва. За таких умов зазначені суб'єкти змушені сегментувати сфери інформаційного середовища, в яких у наступному будуть виконувати необхідну їм інформаційну діяльність.

Таким чином, сфера інформаційної уваги суб'єкта підприємництва являє собою сегмент інформаційного середовища, в якому він забезпечує стратегічні, тактичні та оперативні інформаційні інтереси і завдання.

Звичайно, що інформація у сферах інформаційної уваги суб'єктів підприємництва, як і взагалі в інформаційному їх середовищі існує не взагалі, а зосереджена в певних місцях, які прийнято називати об'єктами інформації.

Об'єктами інформації для кожного суб'єкта підприємництва можна вважати інших суб'єктів, установи засобів масової інформації, установи, організації клієнтів, контрагентів, партнерів, громадські та політичні організації, органи влади та їх установи, науково-дослідні установи, правоохоронні органи і судові установи, детективні та охоронні агентства і організації, рекламні агентства, з'їзди, конференції, виставки, презентації тощо.

Таким чином, організовуючи ІАР суб'єкти підприємництва мають визначатись не тільки із сферами інформаційної уваги, а і з об'єктами інформації, та її джерелами, які з об'єктів та джерел мають представляти для них найбільший інтерес. Водночас, важливим залишається завдання

отримання інформації. Як правило, служби безпеки суб'єктів підприємництва для отримання інформації з відкритих джерел формують так звані інформаційні канали, по яких інформація і потрапляє до суб'єктів**. Під інформаційним каналом** зазвичай розуміють сукупність джерел інформації, засобів та методів їх подання до споживачів інформаційних продуктів.

Використовуючи наявні інформаційні канали суб'єкти підприємництва зосереджують увагу переважно на двох формах збору інформації: інформаційному аудиті і інформаційному моніторингу.

Інформаційний аудит – це інформаційне обстеження сфери інформаційної уваги чи певних об'єктів з метою отримання, вивчення і оцінки необхідної суб'єкту підприємництва інформації. Основними технологіями інформаційного аудиту є: пошук та вивчення інформації про конкретну подію, факт, особу безпосередньо на самому об'єкті; пошук та вивчення інформації про конкретний об'єкт через його зв'язки (ділові, комерційні, організаційні та ін.); пошук та вивчення інформації про конкретний об'єкт шляхом спеціального обстеження його інформаційного середовища. Зміст операцій по кожній з технологій подано в Додатку 6.

Інформаційний моніторинг – це контроль надходження інформації в інформаційне середовище суб'єкта підприємництва з метою виявлення важливої та цінної інформації і її використання для забезпечення його діяльності.

Технологіями, які використовуються в ході інформаційного моніторингу є: контроль інформації, яка надходить в інформаційне середовище суб'єкта підприємництва за визначеними ознаками та індикаторами; контроль інформації, яка надходить в інформаційне середовище суб'єкта по визначених джерелах; суцільний контроль інформації, яка з'являється в інформаційному середовищі суб'єкта.

Основними методами збору інформації в діяльності суб'єктів підприємництва є:

– систематизація інформації, яка надходить до суб'єктів підприємництва від їх клієнтів, споживачів, контрагентів, інших суб'єктів. Ретельне вивчення інформації, отриманої від зазначених джерел про їх стан та діяльність, зв'язки, історію, є досить важливим моментом у зборі інформації та формуванні інформаційного ресурсу;

– надання інформаційних запитів до відповідних установ і організацій та отримання відповіді на них;

– робота з рекламними та пропагандистськими матеріалами, різного роду оголошеннями;

– періодичне опитування, що проводиться суб'єктами підприємництва у їх сегменті ринку;

– постійна робота з друкованими засобами інформації.

Інформація, яка зібрана суб'єктом підприємництва в процесі формування інформаційного ресурсу являє собою відомості, що потребують подальшої обробки.

Структура процесу аналітичної обробки інформації подана на рис. 6.2.

Сформовані висновки та пропозиції надаються керівництву та іншим особам у вигляді інформаційних документів. На даний час за досвідом підприємницької діяльності серед **інформаційних документів** існують:

– інформаційні повідомлення – надання інформації, особливо важливого значення у вигляді усного чи письмового викладення;

– інформаційні доповіді – комплексне і всебічне викладення проблеми з використанням всієї наявної по ній інформації;

– інформаційні довідки – опис окремих характеристик конкретних подій або об'єктів;

– інформаційні огляди – опис основних інформаційних повідомлень за визначений період у формі резюме з класифікацією по рубриках;

– інформаційні зведення – опис загальної картини існуючих подій;

– інформаційні прогнози – короткий огляд подій, фактів, викладення висновків за їх наслідками і можливому розвитку ситуації з відповідним обґрунтуванням.

Аналітичні та інші матеріали, документи, що складають інформаційний ресурс зберігаються у справах поточного та архівного зберігання.

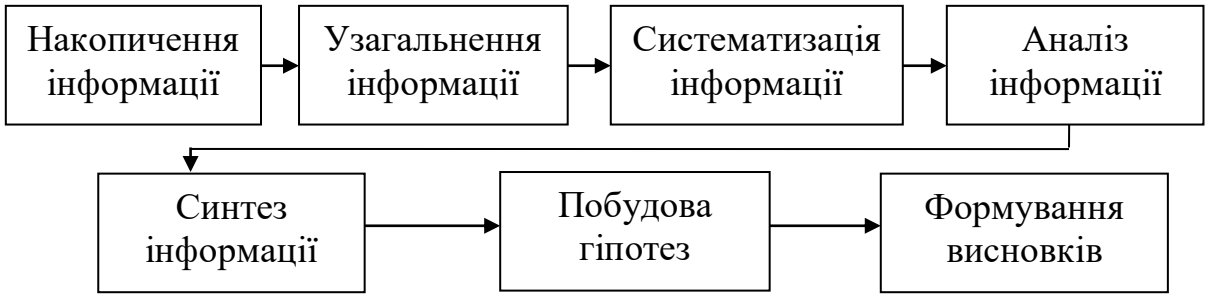

Рис. 6.2. Структура та алгоритм процесу аналітичної обробки інформації

Зазвичай суб'єкти підприємництва створюють електронні бази даних, куди надається інформація про різні сфери їх діяльності та інтересів, клієнтів, партнерів, кредиторів, контрагентів, а також персонал. Звичайно, що і електронні бази даних, і досьє та картотеки, а також поточні та архівні справи відповідним чином захищаються від несанкціонованого доступу до них.

6.3. Спеціальні інформаційні операції та комерційна розвідка в діяльності підприємства

Важливим завданням інформаційної роботи суб'єктів підприємництва в сучасних умовах є забезпечення впливу на його інформаційне середовище з метою формування позитивного іміджу суб'єктів на ринку, маскування роботи по розробці нових продуктів та дезінформації конкурентів чи кримінальних елементів у разі реального існування загроз від них. Забезпечення інформаційного впливу здійснюється шляхом проведення спеціальних інформаційних операцій.

Під **спеціальними інформаційними операціями**, розуміється комплекс спеціальних інформаційних заходів, які проводяться суб'єктами підприємництва протягом конкретно визначеного часу в їх інформаційному середовищі з метою формування (підтримання, відновлення) позитивного іміджу, захисту від негативного інформаційного впливу та дезорієнтації конкурентів та кримінальних елементів, які є суб'єктами загроз.

Тобто, спеціальні інформаційні операції проводяться для забезпечення вигідного положення суб'єктів підприємництва на ринку, особливо при необхідності вирішення важливих для них завдань; формування сприятливої громадської думки про них, їх керівництво і персонал, укріплення (підвищення, відновлення) авторитету суб'єктів і довіри до них з боку партнерів і клієнтів; стратегічної і тактичної дезінформації конкурентів, опонентів та інших суб'єктів, від яких можуть надходити (надходять) загрози.

Видами спеціальних інформаційних операцій є:

– пропаганда – систематичне та активне поширення в інформаційному середовищі інформації про досягнення, переваги, масштаби діяльності суб'єкта підприємництва, вигідність взаємовідносин з ним по різних напрямах його діяльності з метою впливу на суспільну думку і формування позитивного його іміджу. Особливістю пропаганди є те, що вона стосується не продукції суб'єкта підприємництва, а так званого його бренду, комерційного найменування. Тобто пропагується певна ідеологія поведінки на ринку, з чим якраз і пов'язується високий результат. У пропаганді використовуються пропагандистські та агітаційні матеріали: листівки, буклети, відеоматеріали, публікації ЗМІ тощо;

– контрпропаганда – інформаційна реакція суб'єктів підприємництва на комунікативні дії конкурентів чи інших осіб, якими вони прагнуть забезпечити свій вплив на інформаційне середовище ринку всупереч інтересам зазначених суб'єктів.

Безумовно, що контрпропаганда проводиться з метою зниження ефективності заходів пропаганди, які використовуються конкурентами, особливо у випадках коли від таких заходів страждає імідж суб'єктів підприємництва та падає їх конкурентоздатність.

Основними принципами контрпропаганди мають бути активність, оперативність, конкурентність, комплексність, гнучкість, врахування особливостей аудиторії;

– дезінформація — поширення в інформаційному середовищі суб'єктів підприємництва викривлених або неправдивих відомостей з метою введення в оману конкурентів, кримінальних елементів, інших осіб і організацій, що загрожують суб'єктам. Поширена інформація має замаскувати істинні наміри діяльності суб'єктів підприємництва. Захист інтересів суб'єктів підприємництва за допомогою актів дезінформації може здійснюватись по різних напрямах, виходячи з особливостей ситуації, в якій в той чи інший період своєї діяльності знаходиться певний суб'єкт. Зокрема такими напрямками можуть бути:

– введення в оману конкурентів стосовно термінів проведення суб'єктами заходів по підвищенню своєї конкурентоспроможності, надання на ринок нових товарів, послуг, проведення реорганізації і т. і.;

– створення ілюзії підготовки до отримання (вкладання) великих інвестицій в певні сфери економіки чи регіони або інвестування конкретних суб'єктів;

– широке висвітлення «проблем» у суб'єктів підприємництва в окремих сферах їх діяльності, критика низької якості продукції, послуг, робіт;

– «витік» спеціально занижених чи завищених економічних чи інших показників діяльності суб'єктів підприємництва, перебільшення чи заниження негативного впливу політичних, соціальних, економічних або інших умов на перспективи розвитку певних напрямів їх діяльності;

– чутки — усна інформація з невизначеним ступенем достовірності, що стихійно поширюється в інформаційному середовищі суб'єктів підприємництва з метою захисту їх інтересів на ринку. Чутки є неформальним каналом комунікації, по якому можна отримати до 80 % інформації, яка в окремих випадках не суттєво суперечить об'єктивній ситуації. Оскільки чутками інформація передається значно швидше, ніж каналами формального спілкування, суб'єкти підприємництва можуть формувати необхідні їм чутки для запланованого поширення в інформаційне середовище необхідних їм відомостей. Контролюючи зворотню реакцію на чутки суб'єкти можуть коригувати свою діяльність, плани та поведінку на ринку.

Сьогодні багато розмов точиться навколо розвідувальної діяльності в бізнесі. Можна чути про конкурентну, ділову, економічну, комерційну розвідку, бізнес-розвідку, промислове шпигунство тощо. Разом з тим, всі ці назви розкривають одну і ту ж діяльність – отримання необхідної для діяльності суб'єктів підприємництва інформації з джерел, доступ до яких обмежено.

В деяких країнах законодавство щодо захисту інформації є недосконалим (в тому числі і в Україні) і професійні розвідники знаходять шляхи отримання таємної інформації насамперед через прогалини в правових нормах із захисту інформації та прогалини в організації захисту своїх таємниць їх власниками. Основною ж особливістю розвідувальної діяльності є не стільки правомірність її дій щодо проникнення до інформації з обмеженим доступом, а якраз таємний її характер.

Незважаючи на існуючі умови щодо розвідувальної діяльності у бізнесі, певна частина суб'єктів підприємництва все ж таки вдається до відповідних заходів розвідувального характеру. Інформація ж, яку отримують суб'єкти підприємництва в результаті дій їх сил розвідки носить здебільшого комерційний характер і використовується насамперед для забезпечення їх комерційної діяльності. Основним змістом цієї інформації є характеристика ділових стосунків конкурентів, інших суб'єктів, перспективи їх поведінки на ринку, наміри в комерційній діяльності.

Діям сил розвідки суб'єктів підприємництва, які пов'язані із забезпеченням комерційної їх діяльності (що і є предметом підприємництва) більш притаманна назва комерційної розвідки. А оскільки такі дії мають місце у

вітчизняному бізнесі, може бути корисним розгляд деяких аспектів розвідувального забезпечення суб'єктів підприємництва. Тут слід звернути увагу на те, що до професійних дій з розвідки вдаються зазвичай суб'єкти великого бізнесу, оскільки їх можливості дають змогу забезпечити таку діяльність як професійно та матеріально, так певним чином і з правової точки зору.

Враховуючи, що отримання інформації з обмеженим доступом відповідно до чинного законодавства може бути здійснено лише з дозволу її власника, силам розвідки необхідно провести відповідну роботу з ним, розпорядником чи принаймні володільцем такої інформації. В арсеналі розвідки достатньо методів формування позитивних для неї відносин з подібними суб'єктами і як показує практика, доволі часто вдається отримати доступ до інформації, яка цікавить суб'єктів підприємництва.

Слід також звернути увагу і на норми чинного законодавства, які визначають умови доступу до інформації, що є конфіденційною чи таємною. Так, згідно ст. 162 Господарського кодексу України особа, яка самостійно і добросовісно одержала інформацію, що є комерційною таємницею, має право використовувати цю інформацію на свій розсуд.

Основними принципами розвідки в діяльності суб'єктів підприємництва можна вважати: здійснення заходів розвідки в межах чинного законодавства; добування інформації силам розвідки без порушення прав, свобод, честі і гідності громадян; використання добутої інформації виключно в комерційних інтересах; виконання заходів розвідки на професійних засадах.

Середовище комерційної розвідки можуть складати посередники, клієнти, конкуренти, контрагенти, кредитори та інвестори, громадські та політичні об'єднання. Ключовим моментом у комерційній розвідці є інформаційно-пошукова робота, яка може розумітись як комплекс соціальних заходів, спрямованих на виявлення місць зосередження необхідної інформації та її джерел, формування умов та забезпечення процесу отримання інформації.

В умовах відсутності правового регулювання здійснення комерційної розвідки основними її способами можуть бути:

– вивчення наявної інформації;

– опитування;

– спостереження;

– огляд;

– отримання довідок;

– використання спеціальних програм пошуку необхідної інформації в глобальному інформаційному середовищі;

– співпраця з фахівцями, експертами, консультантами,;

– фото- відео зйомка;

– вивідування інформації;

– оманливі перемовини з працівниками об'єктів інформації тошо.

Комерційна розвідка в діяльності суб'єктів підприємництва являє собою певну систему збору, обробки, аналізу, зберігання та використання інформації, класифікації ознак загроз та криз, які можуть зачіпати діяльність суб'єктів і

негативно впливати на їх розвиток, систематизацію таких ознак і розробка на їх основі прогнозів можливого розвитку ситуацій в яких суб'єкти здійснюють свою діяльність або подій, що відбуваються за їх участю.

Актуальність комерційної розвідки в сьогоднішніх умовах обумовлюється насамперед тим, що при наявності великого обсягу інформації, необхідної для прийняття управлінських рішень керівники суб'єктів підприємництва користуються даними і оцінками наданими їм їх менеджерами. В той же час, менеджери, будучи працівниками функціональних підрозділів, як правило, проінформовані одностороннє і зазвичай не мислять категоріями загальних інтересів компанії (фірми, підприємства, банку). Звідси кожен з таких менеджерів прагне підкреслити їх точку зору як найбільш об'єктивну і не помічати деталі, які з їх погляду не варті уваги, оскільки не торкаються функцій їх підрозділів. За таких умов керівники суб'єктів підприємництва попадають у інформаційну залежність від своїх менеджерів і не маючи об'єктивних критеріїв оцінки цінності наданої їм інформації, приймають не зовсім ефективні рішення. Таким недоліком не страждає комерційна розвідка, оскільки є нейтральною до всіх підрозділів, напрямків діяльності суб'єктів підприємництва та позицій менеджерів.

Важливе місце у ІАР займає інформування керівництва та працівників суб'єктів підприємництва.

Основними вимогами до процедури інформування є: відповідність потребам осіб, яким надається інформація, конкретність, обґрунтованість, достовірність, своєчасність, зручна форма і зрозумілість інформації.

Інформаційне забезпечення діяльності суб'єктів підприємництва є важливою умовою сучасного їх функціонування, суттєвим елементом їх безпеки та головною підставою високого статусу на ринку. Водночас інформаційне забезпечення є досить складним, трудомістким видом діяльності, який вимагає до себе постійної уваги.

ТЕМА 7
ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

7.1. Сутність та основні поняття політики безпеки
7.2. Дискреційна політика безпеки
7.3. Мандатна політика безпеки
7.4. Рольова політика безпеки
7.5. Трьохрівнева політика інформаційної безпеки

7.1. Сутність та основні поняття політики безпеки

Фундаментальним поняттям захисту інформації є політика безпеки **(ПБ) або політика захисту**. Важливість цього поняття важко переоцінити – існують ситуації, коли правильно сформульована політика є чи не єдиним механізмом захисту від несанкціонованого доступу.

Сучасне підприємство повинно вміти належним чином будувати політику інформаційної безпеки, тобто розробляти і ефективно впроваджувати комплекс превентивних заходів шодо захисту конфіденційних даних та інформаційних процесів. Така політика повинна передбачати відповідні вимоги до персоналу, менеджерів і технічних служб.

Політика інформаційної безпеки – набір вимог, правил, обмежень, рекомендацій, які регламентують порядок інформаційної діяльності підприємства і спрямовані на досягнення і підтримку стану інформаційної безпеки підприємства.

Політика інформаційної безпеки – документ, що містить принципи діяльності підприємства щодо забезпечення інформаційної безпеки. Цей документ містить перелік загроз, визначає бажаний рівень захищеності, описує організаційні рішення, необхідні для виконання завдань. Задокументована політика інформаційної безпеки – це комплексний план захисту інформації на підприємстві, який покликаний забезпечити фінансово-економічну безпеку підприємства.

Мета політики інформаційної безпеки – впровадження та ефективне управління системою забезпечення інформаційної безпеки, спрямованої на:

– захист інформаційних активів підприємства;
– забезпечення стабільної діяльності підприємства;
– мінімізації ризиків інформаційної безпеки;
– створення позитивних для підприємства інформаційних відносин з партнерами, клієнтами та всередині підприємства.

Політика розповсюджується на всі аспекти діяльності підприємства як інформаційної системи та застосовується до всіх активів підприємства, які можуть здійснювати певний ефект на важливі для існування підприємства об’єкти своєю відсутністю чи псуванням.

Під час розробки політики безпеки мають бути враховані технологія зберігання, обробки та передавання інформації, моделі порушників і загроз, особливості апаратно-програмних засобів, фізичного середовища та інші чинники. На підприємстві може бути реалізовано декілька різних політик

безпеки, які істотно відрізняються одна від одної.

Політика безпеки повинна передбачати використання всіх можливих заходів захисту інформації, як-то: правові та морально-етичні норми, організаційні (адміністративні), фізичні, технічні (апаратні і програмні) заходи – і визначати правила та порядок застосування в організації кожного з цих видів.

Важливо, щоб політика безпеки була сформована на таких основних принципах:

– системності;

– комплексності;

– неперервності захисту;

– достатності механізмів і заходів захисту та їхньої адекватності загрозам;

– гнучкості керування системою захисту, простоти і зручності її використання;

– відкритості алгоритмів і механізмів захисту, якщо інше не передбачено.

Політика безпеки повинна доказово давати гарантії щодо:

– забезпечення адекватності рівня захисту інформації рівню її критичності;

– рентабельної реалізації заходів для захисту інформації;

– забезпечення оцінювання і перевірки захищеності інформації;

– забезпечення персоніфікації положень політики безпеки (стосовно суб'єктів організації), звітності (реєстрація, аудит) для всіх критичних, з точки зору безпеки, ресурсів, до яких здійснений доступ у процесі функціонування інформаційної системи;

– забезпечення персоналу і користувачів достатньо повним комплектом документації стосовно порядку забезпечення захисту інформації;

– створення відповідних планів забезпечення неперервної роботи та її поновлення у разі виникнення непередбачених ситуацій для всіх критичних, з точки зору безпеки інформації, технологій (функцій) організації;

– врахування вимог усіх документів, які регламентують порядок захисту інформації в організації.

Політику безпеки розробляють на підготовчому етапі створення системи забезпечення інформаційної безпеки організації.

Методологія розробки політики безпеки організації включає в себе наступні роботи:

– розробка концепції безпеки інформації в організації;

– аналіз ризиків;

– визначення вимог до заходів, методів та засобів захисту;

– вибір основних рішень із забезпечення безпеки інформації;

– організація виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

– документальне оформлення політики безпеки.

Необхідність у політиці безпеки на сьогоднішній день є очевидним

фактом для будь-якого, навіть невеликого підприємства. Політика безпеки загалом – це сукупність програмних, апаратних, організаційних, адміністративних, юридичних, фізичних заходів, методів, засобів, правил і інструкцій, які чітко регламентують усі аспекти діяльності підприємства, включаючи інформаційну систему, та забезпечують їх безпеку.

Формальний вираз політики безпеки називають **моделлю політики безпеки.**

Основна мета створення політики безпеки інформаційної системи й опису її у вигляді формальної моделі – це визначення умов, яким має підпорядковуватися поведінка системи, вироблення критерію безпеки і проведення формального доведення відповідності системи цьому критерію при додержанні встановлених правил і обмежень.

Незважаючи на те, що створення формальних моделей вимагає суттєвих витрат, вони складні для розуміння і вимагають певної інтерпретації для застосування в реальних системах.

Політика безпеки задається у вигляді правил, відповідно до яких мають виконуватися всі взаємодії між суб'єктами та об'єктами. Взаємодії, що призводять до порушень цих правил, припиняються засобами контролю доступу й не можуть бути здійснені.

7.2. Дискреційна політика безпеки

Основою дискреційної політики безпеки (ДПБ) є дискреційне управління доступом (Discretionary Access Control – DAC), яке визначається двома властивостями:

– усі суб'єкти й об'єкти мають бути однозначно ідентифіковані;

– права доступу суб'єкта до об'єкта системи визначаються на основі певних зовнішніх відносно системи правил.

Назва пункту є дослівним перекладом з англійської терміна Discretionary policy, ще один варіант перекладу – розмежувальна політика. Ця політика одна з найпоширеніших в світі, в системах по замовчуванню мається на увазі сааме ця політика. ДПБ реалізується за допомогою матриці доступу (access matrix), яка фіксує множину об'єктів та суб'єктів, доступних кожному суб'єкту.

Існує декілька варіантів задання матриці доступу:

1. Листи можливостей (privilege list, profile): для кожного суб'єкта створюється лист (файл) усіх об'єктів, до яких має доступ даний суб'єкт.

2. Листи контролю доступу (access control list): для кожного об'єкта створюється список усіх суб'єктів, що мають доступи до цього об'єкта.

До переваг ДПБ можна віднести відносно просту реалізацію відповідних механізмів захисту. Саме цим зумовлено той факт, що більшість поширених нині захищених автоматизованих систем забезпечують виконання положень саме ДПБ. Однак багатьох проблем захисту ця політика розв'язати не може.

Наведемо найбільш суттєві вади ДПБ:

1. Один з найбільших недоліків цього класу політик – вони не витримують атак за допомогою «Троянського коня». Це, зокрема, означає, що

система захисту, яка реалізує ДПБ, погано захищає від проникнення вірусів у систему та інших способів прихованої руйнівної дії.

2. Автоматичне визначення прав. Оскільки об'єктів багато і їх кількість безперервно змінюється, то задати заздалегідь вручну перелік прав кожного суб'єкта на доступ до об'єктів неможливо. Тому матриця доступу різними способами агрегується, наприклад, суб'єктами залишаються тільки користувачі, а у відповідну клітину матриці вставляються формули функцій, обчислення яких визначає права доступу суб'єкта, породженого користувачем, до об'єкта.

Звичайно, ці функції можуть змінюватися з часом. Зокрема, можливе вилучення прав після виконання певної події, також можливі модифікації, що залежать від інших параметрів.

3. Контроль поширення прав доступу. Найчастіше буває так, що власник файла передає вміст файла іншому користувачеві і той відповідно набуває права власника на цю інформацію. Отже, права можуть поширюватись, і навіть якщо перший власник не хотів передати доступ іншому суб'єкту до своєї інформації, то після кількох кроків передача прав може відбутися незалежно від його волі. Виникає задача про умови, за якими в такій системі певний суб'єкт рано чи пізно отримає необхідний йому доступ.

4. При використанні ДПБ виникає питання визначення правил поширення прав доступу й аналізу їх впливу на безпеку АС. У загальному випадку при використанні ДПБ органом, який її реалізує і який при санкціонуванні доступу суб'єкта до об'єкта керується певним набором правил, стоїть задача, яку алгоритмічно неможливо розв'язати: перевірити, призведуть його дії до порушень безпеки чи ні. Отже, матриця доступів не є тим механізмом, який дозволив би реалізувати ясну і чітку систему захисту інформації в автоматизованій системі. Більш досконалою політикою виявилася мандатна політика безпеки.

7.3. Мандатна політика безпеки

Основу мандатної (повноважної) політики безпеки (МПБ) становить мандатне управління доступом (Mandatory Access Control – MAC), яке передбачає, що:

– всі суб'єкти й об'єкти повинні бути однозначно ідентифіковані;

– у системі визначено лінійно упорядкований набір міток секретності;

– кожному об'єкту системи надано мітку секретності, яка визначає цінність інформації, що міститься в ньому, – його рівень секретності в АС;

– кожному суб'єкту системи надано мітку секретності, яка визначає рівень довіри до нього в АС – максимальне значення мітки секретності об'єктів, до яких суб'єкт має доступ; мітка секретності суб'єкта називається його рівнем доступу.

Основна мета МПБ – запобігання витоку інформації від об'єктів з високим рівнем доступу до об'єктів з низьким рівнем доступу, тобто протидія виникненню в АС інформаційних каналів згори вниз. Вона оперує, таким чином, поняттями інформаційного потоку і цінності інформаційних об'єктів. Цінність інформаційних об'єктів (або їх мітки рівня секретності) часто дуже

важко визначити. Однак досвід показує, що в будь-якій АС майже завжди для будь-якої пари об'єктів X та *Y* можна сказати, який з них більш цінний.

Тобто, можна вважати, що таким чином фактично визначається деяка однозначна функція *c(X),* яка дозволяє для будь-яких об'єктів *X* і *Y* сказати, що коли *Y* більш цінний об'єкт, ніж *X*, то *c(Y) > c(X).* І навпаки, якщо *c(Y) > c(X),* то *Y* – більш цінний об'єкт, ніж *X*. Тоді потік інформації від *X* до *Y* дозволяється, якщо *c(X) < c(Y),* і не дозволяється, якщо *c(X) > c(Y).*

Отже, МПБ має справу з множиною інформаційних потоків, яка ділиться на дозволені і недозволені за дуже простою умовою – значенням наведеної функції. МПБ у сучасних системах захисту на практиці реалізується мандатним контролем на найнижчому апаратно-програмному рівні, що дає змогу досить ефективно будувати захищене середовище для механізму мандатного контролю.

Пристрій мандатного контролю називають монітором звернень. Мандатний контроль, який ще називають обов'язковим, оскільки його має проходити кожне звернення суб'єкта до об'єкта, організується так: монітор звернень порівнює мітки рівня секретності кожного об'єкта з мітками рівня доступу суб'єкта. За результатом порівняння міток приймається рішення про допуск.

Найчастіше МПБ описують у термінах, поняттях і визначеннях властивостей моделі Белла-Лападула. У рамках цієї моделі доводиться важливе твердження, яке вказує на принципову відмінність систем, що реалізують мандатний захист, від систем з дискреційним захистом: «якщо початковий стан системи безпечний і всі переходи системи зі стану до стану не порушують обмежень, сформульованих ПБ, то будь-який стан системи безпечний».

Наведемо ряд переваг МПБ порівняно з ДПБ:

1. Для систем, де реалізовано МПБ, є характерним вищий ступінь надійності. Це пов'язано з тим, що за правилами МПБ відстежуються не тільки правила доступу суб'єктів системи до об'єктів, а й стан самої АС. Таким чином, канали витоку в системах такого типу не закладені первісно (що є в положеннях ДПБ), а можуть виникнути тільки при практичній реалізації систем внаслідок помилок розробника.

2. Правила МПБ ясніші і простіші для розуміння розробниками і користувачами АС, що також є фактором, який позитивно впливає на рівень безпеки системи.

3. МПБ стійка до атак типу «Троянський кінь».

4. МПБ допускає можливість точного математичного доведення, що система в заданих умовах підтримує ПБ.

Однак МПБ має дуже серйозні вади – вона дуже складна для практичної реалізації і вимагає значних ресурсів АС. Це пов'язано з тим, що інформаційних потоків у системі величезна кількість і їх не завжди можна ідентифікувати. Саме ці вади часто заважають її практичному використанню.

МПБ прийнята всіма розвинутими державами світу. Вона розроблялася, головним чином, для збереження секретності (тобто конфіденційності) інформації у військових організаціях. Питання ж цілісності за її допомогою не

розв’язуються або розв’язуються частково, як побічний результат захисту секретності.

7.4. Рольова політика безпеки

Рольову політику безпеки (РПБ) (Role Base Access Control – RBAC) не можна віднести ані до дискреційної, ані до мандатної, тому що керування доступом у ній здійснюється як на основі матриці прав доступу для ролей, так і за допомогою правил, які регламентують призначення ролей користувачам та їх активацію під час сеансів. Отже, рольова модель є цілком новим типом політики, яка базується на компромісі між гнучкістю керування доступом, характерною для ДПБ, і жорсткістю правил контролю доступу, що притаманна МПБ.

У РПБ класичне поняття «суб’єкт» заміщується поняттями «користувач» і «роль».

Користувач – це людина, яка працює з системою і виконує певні службові обов’язки.

Роль – це активно діюча в системі абстрактна сутність, з якою пов’язаний обмежений, логічно зв’язаний набір повноважень, необхідних для здійснення певної діяльності.

РПБ застосовується досить широко, тому що вона, на відміну від інших більш строгих і формальних політик, є дуже близькою до реального життя.

Справді, по суті, користувачі, що працюють у системі, діють не від свого власного імені – вони завжди виконують певні службові обов’язки, тобто виконують деякі ролі, які аж ніяк не пов’язані з їх особистістю. Тому цілком логічно здійснювати керування доступом і призначати повноваження не реальним користувачам, а абстрактним (не персоніфікованим) ролям, які представляють учасників певного процесу обробки інформації. Такий підхід до ПБ дозволяє врахувати розподіл обов’язків і повноважень між учасниками прикладного інформаційного процесу, оскільки з точки зору РПБ має значення не особистість користувача, користувача, що здійснює доступ до інформації, а те, які повноваження йому необхідні для виконання його службових обов’язків.

Наприклад, у реальній системі обробки інформації можуть працювати системний адміністратор, менеджер баз даних і прості користувачі. У такій ситуації РПБ дає змогу розподілити повноваження між цими ролями відповідно до їх службових обов’язків: ролі адміністратора призначаються спеціальні повноваження, які дозволять йому контролювати роботу системи і керувати її конфігурацією, роль менеджера баз даних дозволяє здійснювати керування сервером БД, а права простих користувачів обмежуються мінімумом, необхідним для запуску прикладних програм. Крім того, кількість ролей у системі може не відповідати кількості реальних користувачів – один користувач, якщо він має різні повноваження, може виконувати (водночас або послідовно) кілька ролей, а кілька користувачів можуть користуватися однією й тією ж роллю, якщо вони виконують однакову роботу.

При використанні РПБ керування доступом здійснюється в дві стадії: по-перше, для кожної ролі вказується набір повноважень, що представляють набір

прав доступу до об’єктів, і, по-друге, кожному користувачеві призначається список доступних йому ролей. Повноваження призначаються ролям відповідно до принципу найменших привілеїв, з якого випливає, що кожний користувач повинен мати тільки мінімально необхідні для виконання своєї роботи повноваження.

У моделі РПБ визначаються множини:

– множина користувачів;

– множина ролей;

– множина повноважень на доступ до об’єктів, наприклад, у вигляді матриці прав доступу;

– множина сеансів роботи користувачів з системою.

Для перелічених множин визначаються відношення, які встановлюють для кожної ролі набір наданих їй повноважень, а також для кожного користувача – набір доступних йому ролей.

Правила керування доступом РПБ визначаються певними функціями, які для кожного сеансу визначають користувачів, набір ролей, що можуть бути одночасно доступні користувачеві в цьому сеансі, а також набір доступних у ньому повноважень, що визначається як сукупність повноважень усіх ролей, що беруть участь у цьому сеансі.

Як критерій безпеки рольової моделі використовується правило: «система вважається безпечною, якщо будь-який користувач системи, що працює в певному сеансі, може здійснити дії, які вимагають певних повноважень тільки в тому випадку, коли ці повноваження належать сукупності повноважень усіх ролей, що беруть участь у цьому сеансі».

З формулювання критерію безпеки рольової моделі випливає, що управління доступом здійснюється, головним чином, не за допомогою призначення повноважень ролям, а шляхом встановлення відношення, яке призначає ролі користувачам, і функції, що визначає доступний у сеансі набір ролей. Тому численні інтерпретації рольової моделі відрізняються видом функцій, що визначають правила керування доступом, а також обмеженнями, що накладаються на відношення між множинами.

Завдяки гнучкості та широким можливостям РПБ суттєво перевершує інші політики, хоча іноді її певні властивості можуть виявитися негативними. Так, вона практично не гарантує безпеку за допомогою формального доведення, а тільки визначає характер обмежень, виконання яких і є критерієм безпеки системи. Хоча такий підхід дозволяє отримати прості й зрозумілі правила контролю доступу (перевага), які легко застосовувати на практиці, проте позбавляє систему теоретичної доказової бази (вада).

У деяких ситуаціях ця обставина утруднює використання РПБ, однак у кожному разі оперувати ролями набагато зручніше, ніж суб’єктами (знову перевага), оскільки це більше відповідає поширеним технологіям обробки інформації, які передбачають розподіл обов’язків і сфер відповідальності між користувачами. Крім того, РПБ може використовуватися одночасно з іншими ПБ, коли повноваження ролей, що призначаються користувачам,

контролюється контролюється ДПБ або МПБ, що дозволяє будувати багаторівневі схеми контролю доступу.

7.5. Трьохрівнева політики інформаційної безпеки

З практичної точки зору політику безпеки доцільно розділити на три рівні. До верхнього рівня можна віднести рішення, що торкаються організації в цілому. Вони носять дуже загальний характер і, як правило, виходять від керівництва організації. Наприклад, список подібних рішень може включати в себе:

– формування або перегляд самої комплексної програми забезпечення інформаційної безпеки, призначення відповідальних за реалізацію цієї програми;

– формулювання цілей у сфері інформаційної безпеки та визначення загальних напрямів їх досягнення;

– забезпечення технічної бази для дотримання відповідних законів і правил;

– формулювання управлінських рішень з тих питань реалізації програмної безпеки, які повинні розглядатися на рівні організації в цілому.

На політику верхнього рівня впливають цілі організації в галузі інформаційної безпеки: вони формулюються, як правило в термінах цілісності, доступності та конфіденційності. Якщо організація відповідає за підтримку критично важливих баз даних, то на першому плані може стояти зменшення випадків втрат, пошкоджень або спотворень даних. Для організації, що займається наданням послуг, імовірно, важлива актуальність інформації про ці послуги та їх ціни, а також доступність послуг максимальному числу потенційних покупців. Режимна організація в першу чергу піклується про захист від несанкціонованого доступу – конфіденційності.

На верхній рівень виноситься управління ресурсами захисту та координація їх використання, виділення спеціального персоналу для захисту особливо важливих систем, підтримка контактів з іншими організаціями, що забезпечують чи контролюють режим безпеки.

Сфера політики верхнього рівня повинна бути чітко окреслена. Можливо, це будуть комп’ютерні системи самої організації, а, можливо, і деякі аспекти використання домашніх комп’ютерів у співробітників цієї організації. Можна уявити собі, і таку ситуацію, коли в сферу впливу включаються лише окремі найбільш важливі системи політики інформаційної безпеки підприємства. Вироблення програми інформаційної безпеки верхнього рівня і її здійснення – це завдання певних посадових осіб, за виконання якої вони повинні регулярно звітувати.

Нарешті, політика інформаційної безпеки верхнього рівня, очевидно, повинна вписуватися в існуючі закони держави, а щоб бути впевненими в тому, що їй точно й акуратно слідує персонал підприємства, доцільно розробити систему відповідних заохочень і покарань. А взагалі-то кажучи, на верхній рівень слід виносити мінімум питань. До середнього рівня можна віднести

окремі аспекти інформаційної безпеки, проте важливі для різних систем, експлуатованих організацією.

Політика середнього рівня по кожному подібному аспекту передбачає вироблення відповідного документованого управлінського рішення, в якому зазвичай є:

– Опис аспекта. Наприклад, якщо взяти застосування користувачами неофіційного програмного забезпечення, то про нього обов'язково має бути сказано, що це таке забезпечення, яке не було схвалено і / або закуплено на рівні організації.

– Вказівка на область її застосування (розповсюдження тієї чи іншої політики інформаційної безпеки). Іншими словами має бути сертифіковано, де, коли, як, по відношенню до кого і чого застосовується дана політика безпеки.

– Чіткий розподіл відповідних ролей та обов'язків. У «політичний» документ необхідно включити інформацію про посадових осіб, відповідальних за проведення політики безпеки в життя. Наприклад, якщо для використання працівником неофіційного програмного забезпечення потрібно офіційний дозвіл, то має бути відомо, у кого і як його слід отримувати. Якщо повинні перевірятися диски, принесені з інших комп'ютерів, необхідно описати процедуру перевірки. Якщо неофіційне програмне забезпечення використовувати не можна, слід знати, хто стежить за виконанням цього правила.

– Механізм забезпечення «законослухняності». Політика має містити загальний опис заборонених дій і покарання за них.

– Вказівки на необхідні «точки контакту». Повинно бути точно відомо, куди слід звертатися за роз'ясненнями, допомогою та додатковою інформацією. Зазвичай «точкою контакту» служить посадова особа.

Політика безпеки нижнього рівня відноситься до конкретних сервісів. Вона включає в себе всього два аспекти – мети і правила їх досягнення, тому її часом важко відокремити від питань реалізації (надання послуг з інформаційного забезпечення). На відміну від двох верхніх рівнів, розглянута політика нерідко буває набагато більш детальною. Є багато питань, специфічних для окремих сервісів, які не можна єдиним чином регламентувати в рамках всієї організації. У той же час ці питання настільки важливі для забезпечення режиму безпеки, що рішення, які належать до них, повинні прийматися на управлінському, а не технічному рівні. Ось лише кілька прикладів-запитань, на які слід дати відповідь при розробці політики безпеки нижнього рівня:

– Хто має право доступу до об'єктів, що підтримуються сервісом?

– За яких умов можна читати і модифікувати дані?

– Як організований вилучений доступ до сервісу?

При формулюванні цілей, політика нижнього рівня може виходити з міркувань цілісності, доступності та конфіденційності, але вона не повинна на цьому зупинятися. Її цілі мають бути конкретнішими. Наприклад, якщо мова йде про систему розрахунку зарплати, можна поставити мету, щоб тільки працівникам відділу кадрів і бухгалтерії дозволялося вводити і змінювати

інформацію. У більш загальному випадку цілі повинні пов’язувати між собою об’єкти сервісу та логічні з точки зору інформаційної безпеки, осмислені, дії з ними. З цілей зазвичай виводяться правила безпеки, що описують, хто, що і за яких умов може робити. Чим детальніше правила, чим більш формально вони викладені, тим простіше підтримувати їх виконання програмно-технічними заходами. З іншого боку, занадто жорсткі правила можуть заважати роботі користувачів, і, ймовірно, їх доведеться часто переглядати.

Керівництву необхідно знайти розумний компроміс, коли за прийнятну ціну буде забезпечений прийнятний рівень безпеки, а працівники не виявляться надмірно сковані.

ТЕМА 8
УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ НА ПІДПРИЄМСТВІ

8.1. Характеристика інформаційних ризиків на підприємстві

8.2. Аналіз та оцінювання інформаційних ризиків на підприємстві

8.3. Напрями мінімізації інформаційних ризиків у діяльності підприємства

8.1. Характеристика інформаційних ризиків на підприємстві

До інформаційних ризиків відносять всі ризики, пов'язані з небезпекою виникнення збитків або шкоди в результаті застосування підприємством інформаційних технологій.

Інформаційні ризики тісно пов'язані зі створенням, передачею, збереженням і використанням інформації за допомогою електронних носіїв або інших засобів зв'язку.

Загрозу можуть представляти не тільки технічні збої, але і неузгодженість даних у різних системах, а також необмежений доступ працівників до інформації.

Якщо причини виникнення інформаційного ризику знаходяться всередині підприємства, то такі ризики відносять до **внутрішніх**; **зовнішніми** інформаційними ризиками вважають ризики, які виникають внаслідок дії зовнішніх факторів.

За своїм походженням інформаційні ризики поділяються на три категорії:

– ризики, пов'язані з втратою (витоком, руйнуванням, знищенням) інформації. Особливо небезпечним є ризик втрати такої інформації, як комерійної таємниця або іншої інформації з обмеженим доступом;

– ризики, пов'язані з формуванням інформаційного ресурсу (використання неповної, неправдивої інформації, відсутність необхідної інформації, дезінформація): ризики збору інформації, ризики узагальнення і класифікації, ризики обробки інформації, ризики представлення;

– ризики, пов'язані з інформаційним впливом на діяльність підприємств (поширення неправдивої, негативної інформації, інформаційно-психологічний вплив на працівників, клієнтів, інформаційний тероризм).

За якістю інформаційного ресурсу виділяють такі види інформаційних ризиків:

– ризик відсутності необхідної інформації;

– ризик отримання і використання неповної, необ'єктивної інформації;

– ризик спотворення інформації (випадкового чи навмисного) під час обробки;

– ризик дезінформації.

За видом інформаційного впливу на підприємство виділяють такі ризики:

– ризик втрати іміджу;

– ризик конфліктних ситуацій з власним персоналом, клієнтами, акціонерами, державними органами;

– ризик блокування роботи підприємства шляхом численних перевірок його діяльності.

Серед ризиків інформаційного впливу особливу небезпеку становить ризик потрапляння суб'єктів підприємництва під дію інформаційного тероризму. Ураховуючи відчутні наслідки, до яких можуть призвести дії інформаційного тероризму, суб'єкти підприємництва не повинні ігнорувати такий вид ризиків і мають виробляти відповідну політику щодо їх мінімізації.

Інформаційні ризики необхідно розглядати не як окремо взяті, а у сукупності з іншими ризиками підприємницької діяльності. Саме в такий спосіб можна правильно прийняти рішення щодо ризику проведення певної операції чи діяльності загалом: прийняти ризики, тобто погодитися на можливі втрати у процесі негативного впливу ризику; вжити заходів щодо зниження ризику; передати ризик іншому суб'єкту (компенсацію можливих збитків покласти, скажімо, на страхову компанію або трансформувати інформаційний ризик в інші види ризику, з більш низьким рівнем втрат).

Водночас за певних умов інформаційні ризики можуть бути головними серед тих ризиків, яких зазнає суб'єкт підприємництва у своїй діяльності.

8.2. Аналіз та оцінювання інформаційних ризиків на підприємстві

Процес аналізу ризиків складається з декількох етапів – визначення видів ризиків, що можуть з'явитися чи уже з'явилися і впливають на діяльність того або іншого підприємства, оцінки їх впливу на діяльність підприємства та оцінки ймовірної шкоди, що може бути заподіяна внаслідок реалізації цього ризику.

Оцінювання інформаційного ризику передбачає оцінку обсягу шкоди, яку може зазнати суб'єкт унаслідок впливу зазначеного ризику.

Важливою проблемою у діяльності суб'єктів підприємництва є мінімізації втрати інформації. Головним в аналізі ризиків втрати інформації є виявлення способів несанкціонованого доступу до інформації суб'єктів підприємництва та її найбільш уразливих носіїв. Під час проведення такого аналізу слід виходити з того, що інформація може бути зосереджена переважно в двох групах її носіїв: комп'ютерній інформаційній мережі та в працівників суб'єктів підприємництва. Звідси несанкціонований доступ до інформації може бути здійснено, з одного боку, за допомогою технічних і програмних засобів, а з другого – за допомогою засобів інтелектуального та психологічного характеру.

Оцінювання ризиків втрати інформації передбачає оцінку вартості інформаційних ресурсів, щодо яких існує ризик втрати, та оцінку власне самого ризику як імовірності реалізації певної загрози, у даному разі пов'язаної з втратою інформації. Вартість інформації оцінюється через її комерційну цінність, яка визначається через розміри збитків (шкоди), які можуть настати у зв'язку з її втратою, обсягом (перспективами) вигоди, яку може отримати суб'єкт підприємництва, використовуючи наявну в нього інформацію, а також витрати, пов'язані з виробленням, отриманням і захистом такої інформації.

Оцінювання ризиків, пов'язаних з формуванням інформаційного ресурсу, може визначатися через ціну (вартість) певної операції, щодо якої здійснюється інформаційне забезпечення або обсяги прибутку, які може отримати суб'єкт підприємництва у разі прийняття рішення на основі об'єктивної інформації. Тобто, ціна ризику визначається обсягом зроблених суб'єктом вкладень та очікуваного прибутку.

Оцінювання ризиків інформаційного впливу спрямовується на визначення сфери діяльності та взаємовідносин суб'єктів підприємництва, щодо яких може поширюватись негативна для них інформація в той чи інший період їх діяльності і таким чином утворюватися певний ризик.

У процесі **оцінювання ризиків інформаційного тероризму** визначається, які наслідки можуть настати для суб'єктів підприємництва через інформаційні атаки терористів як з погляду економічного, так і з погляду їх іміджу. Тут можна формувати певні прогнози щодо таких наслідків (втрата клієнтів, звільнення провідних працівників з роботи, втрата інформації, що має обмежений доступ, викрадення коштів з рахунків суб'єктів та їх клієнтів, руйнування програмного забезпечення роботи інформаційної мережі та інформаційних систем). Стосовно конкретного виміру обсягу шкоди, завданої від актів інформаційного тероризму, то тут поки що відсутні якісь підходи. Практично неможливо передбачити, а тим більше прорахувати обсяги можливої шкоди від таких дій. Тому під час оцінювання зазначених ризиків обмежуються можливими категоріями наслідків, які можуть наступати у зв'язку з інформаційними атаками терористів.

Існують різні способи оцінювання інформаційних ризиків (рис. 8.1):

– методи;
– управляючі документи;
– інструменти.

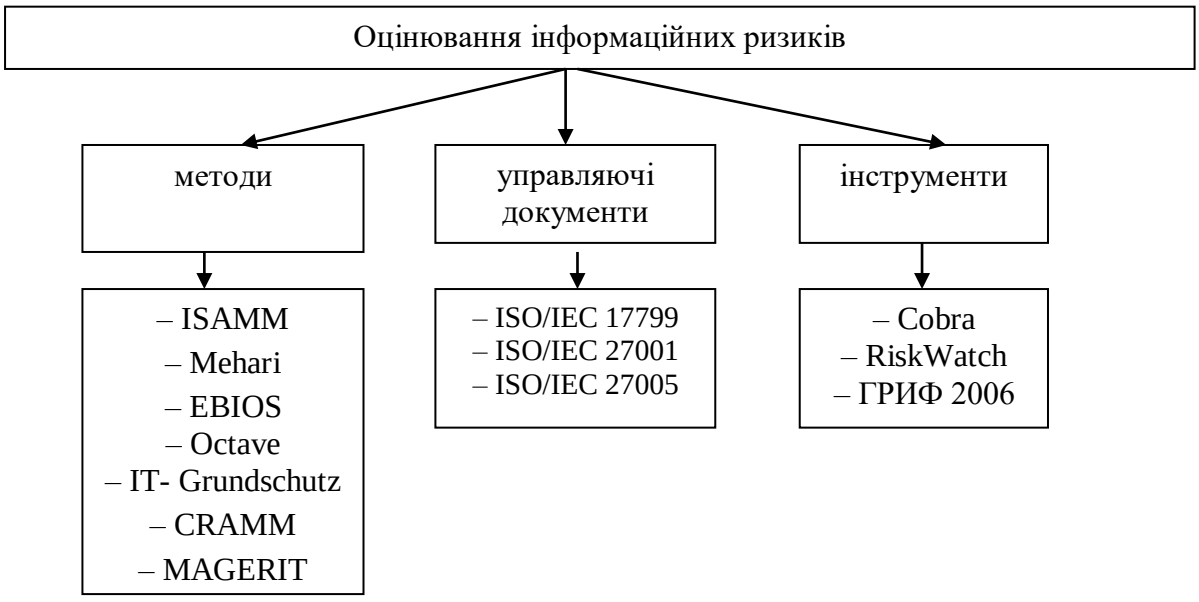

Рис. 8.1. Способи оцінювання інформаційних ризиків

Методи оцінювання інформаційних ризиків поділяються на кількісні, якісні та змішані (комбінація кількісних методів з якісними).

Завдання якісної оцінки – визначення можливих видів ризиків, оцінка принципового рівня серйозності загроз, а також виділення чинників, які впливають на рівень обґрунтування різних можливих контрзаходів. Ці методики не надають кількісні або грошові значення компонентам і втратам. Вони достатньо популярні, відносно прості і розроблені, як правило, на основі вимог міжнародного стандарту ISO/IEC 17799:2005.

Кількісні методики надають реальні й осмислені чисельні значення всім елементам процесу аналізу ризиків. Цими елементами можуть бути вартість захисних заходів, цінність активу, збиток для бізнесу, частота виникнення загрози, ефективність захисних заходів, вірогідність використання уразливості і так далі. Кількісний аналіз дозволяє набути конкретного значення ймовірності (у відсотках) реалізації загрози.

Також доволі часто використовується комбінація цих двох підходів, як правило, на початкових етапах аналізу інформаційних ризиків використовується якісний, а на кінцевому – саме отримання оцінки – кількісний.

1. Найбільш відомі методи оцінювання інформаційних ризиків:

1.1. ISAMM.

Виробник: Бельгія.

Опис: ISAMM була розроблена на основі Telindus. Це кількісний тип методології управління ризиками, де оцінюються ризики, виражаючи їх через щорічні очікувані збитки в грошових одиницях.

Ефективність методу дозволяє виконувати обгрунтовану оцінку ризику в рамках, з мінімальними витратами часу і зусиль. Цей метод оцінювання ризиків складається з трьох основних частин: огляду; оцінки; результат розрахунків та звітність.

Метод оцінки ризику: кількісний.

Наявність допоміжних програмних інструментів: немає, але має хорошу керівну документацію.

1.2. Mehari.

Виробник: Франція.

Опис: Це модель управління ризиками з модульними компонентами і процесами.

Метод оцінки ризику: якісний і кількісний.

Наявність допоміжних програмних інструментів: є.

1.3. EBIOS.

Виробник: Франція.

Опис: Цей метод широко використовується як в державному, так і приватному секторі. EBIOS формалізує підхід до оцінки ризику в області інформаційної безпеки систем. Метод враховує всі технічні об’єкти (програмне і апаратне забезпечення, мережі) і нетехнічні об’єкти (організації, людські аспекти, фізична безпека).

Метод оцінки ризику: якісний.

Наявність допоміжних програмних інструментів: є.

1.4. Octave.

Виробник: США.

Опис: OCTAVE є самостійним підходом, що вказує на те, що персонал несе відповідальність за встановлення стратегії безпеки організації. OCTAVE вимагає аналізу в розгляді відносини між критично важливими активами, загрозами для цих активів і вразливостями (як організаційні, так і технологічні). Він визначає пов'язані з інформацією активи, які важливі для організації і зосереджує діяльність на ці активи, тому що вони мають найбільш важливе значення для організації (акцент на кількох важливих активів, не більше п'яти). Існують різні OCTAVE методи, засновані на OCTAVE критеріях: OCTAVE, OCTAVE-S і OCTAVE Allegro.

Метод оцінки ризику: якісний.

Наявність допоміжних програмних інструментів: є.

1.5. IT-Grundschutz.

Виробник: Німеччина.

Опис: IT-Grundschutz пропонує спосіб для створення системи управління інформаційною безпекою. Вона включає в себе як загальні рекомендації по забезпеченню безпеки IT так і допоміжні технічні рекомендації для досягнення необхідного рівня IT безпеки для конкретного домену.

У методі IT-Grundschutz представлені каталоги: 1) модулі; 2) каталоги загроз; 3) каталоги захисту.

Метод оцінки ризику: якісний.

Наявність допоміжних програмних інструментів: є.

1.6. CRAMM.

Виробник: Великобританія.

Опис: Метод CRAMM досить складно використовувати без CRAMM інструменту. У інструмента такаж назва, як і у методу – CRAMM. В основі методу CRAMM лежить комплексний підхід до оцінки ризиків, поєднуючи кількісні та якісні методи аналізу. Метод є універсальним і підходить як для великих, так і для дрібних організацій, як урядового, так і комерційного сектора. Грамотне використання методу CRAMM дозволяє отримувати дуже хороші результати, найбільш важливим з яких є можливість економічного обгрунтування витрат організації на забезпечення інформаційної безпеки та безперервності бізнесу. Економічно обгрунтована стратегія управління ризиками дозволяє, в кінцевому підсумку, заощаджувати кошти, уникаючи невиправданих витрат.

Метод оцінки ризику: якісний і кількісний.

Наявність допоміжних програмних інструментів: є.

1.7. Назва методу: Magerit.

Виробник: Іспанія.

Опис: Magerit є відкритою методологією аналізу та управління ризиками пропонованої в якості основи і керівництва:

– для того, щоб особи відповідальні за інформаційні системи знали про існування ризиків і необхідность розглядати їх своєчасно;

– для пропозиції систематичного методу аналізу цих ризиків;

– для опису і планування відповідних заходів по утриманню ризику під контролем;

– для підготовки організації по процесу оцінки, аудиту, сертифікації та акредитації.

Метод оцінки ризику: кількісний і якісний.

Наявність допоміжних програмних інструментів: є.

2. Управляючі документи.

Крім методів оцінки ризиків використовують управляючі документи, де теоретично описуються і даються методичні вказівки процесу оцінювання ризиків, але не дається конкретних технологій. Найвідоміші стандарти, які використовуються на території України: ISO 17799, ISO 27001, ISO 27005.

2.1. ISO / IEC 17799 «Інформаційні технології. Методи забезпечення безпеки. Практичні рекомендації менеджменту інформаційної безпеки».

Опис: Стандарт ISO / IEC 17799 надає кращі практичні поради з менеджменту інформаційної безпеки для тих, хто відповідає за створення, реалізацію або обслуговування систем менеджменту інформаційної безпеки. Інформаційна безпека визначається стандартом як «збереження конфіденційності (впевненості в тому, що інформація доступна тільки тим, хто уповноважений мати такий доступ), цілісності (гарантії точності і повноти інформації та методів її обробки) і доступності (гарантії в тому, що уповноважені користувачі мають доступ до інформації та пов'язаних ресурсів).

На основі стандарту ISO / IEC 17799 розроблений в 2005 році стандарт ISO / IEC 27002.

2.2. ISO / IEC 27001 «Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги» (2005р.).

Опис: Міжнародний стандарт ISO / IEC 27001 надає модель для розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та удосконалення документованої системи управління інформаційною безпекою в контексті існуючих бізнес ризиків організації. Стандарт ISO / IEC 27001 являє наочну модель менеджменту, що дозволяє здійснювати оцінку ризиків, проектування і реалізацію системи інформаційної безпеки, її менеджмент і переоцінку.

2.3. ISO / IEC 27005 «Інформаційні технології. Методи і засоби забезпечення безпеки. Управління ризиками інформаційної безпеки» (2008р., наступна редакція 2011р.).

Опис: Цей стандарт призначений для визначення в організації підходу до менеджменту ризиків інформаційної безпеки в залежності, наприклад, від сфери дії СМІБ, сфери застосування менеджменту ризиків або сектора промисловості. Забезпечує рекомендації для менеджменту ризиків інформаційної безпеки, які включають інформацію і менеджмент ризиків безпеки технологій телекомунікації. Стандарт підтримує загальні концепції, визначені в ISO / IEC 27001, і призначений для сприяння адекватного забезпечення інформаційної безпеки на основі підходу, пов'язаного з менеджментом ризику. Застосуємо для організацій усіх типів (наприклад,

комерційних підприємств, державних установ, некомерційних організацій), які планують здійснювати менеджмент ризиків, для компрометації інформаційної безпеки організації.

3. Інструменти.

Крім методів та управляючих документів використовують інструменти для оцінювання ризиків. Інструменти являють собою програмне забезпечення з документацією про правила використання. Найвідомішими інструментами є: Cobra, RiskWatch, ГРИФ 2006.

3.1. Cobra.

Виробник: Великобританія.

Опис: Cobra – програмний інструмент, який дозволяє проводити оцінку ризиків у сфері безпеки. Він оцінює відносну важливість усіх загроз і вразливостей, генерує відповідні рішення та рекомендації. Це автоматично пов'язує виявлені ризики з потенційними наслідками для бізнес-одиниці. Крім того, конкретний район або питання може бути розглянуте «самостійно», без будь-яких наслідків для організації.

3.2. RiskWatch.

Виробник: США.

Опис: RiskWatch являє собою сімейство програмних продуктів, побудованих на загальному програмному ядрі, які призначені для управління різними видами ризиків та підтримки великого різновиду стандартів. У RiskWatch в якості критеріїв для оцінки та управління ризиками використовуються очікувані річні втрати (Annual Loss Expectancy, ALE) та оцінка повернення інвестицій (Return on Investment, ROI). RiskWatch орієнтована на точну кількісну оцінку співвідношення втрат від загроз безпеки і затрат на створення системи захисту.

3.3. ГРИФ 2006.

Виробник: Росія.

Опис: ГРИФ 2006 – потужний і зручний інструмент для аналізу захищеності ресурсів інформаційної системи та ефективного управління ризиками. Дозволяє провести повний аналіз ризиків – отримати повну картину всіх загроз, актуальних для інформаційної системи, оцінити, наскільки критичні уразливості і до яких втрат вони можуть привести. Крім аналізу ризиків, є можливість управління ризиками. Алгоритм системи «ГРИФ 2006» аналізує побудовану модель і генерує звіт, який містить значення ризику для кожного ресурсу. Конфігурація звіту може бути практично будь-якою, таким чином, дозволяючи створювати як короткі звіти для керівництва, так і детальні звіти для подальшої роботи з результатами.

8.3. Напрями мінімізації інформаційних ризиків у діяльності підприємства

Мінімізація інформаційних ризиків передбачає вжиття заходів, спрямованих на зниження ймовірності негативного впливу ризиків, їх уникнення або зменшення їх обсягу.

Для зниження (мінімізації) ризику втрати інформації суб'єкти підприємництва мають вживати відповідних заходів, диференціюючи їх відповідно до певних загроз. Серед таких заходів насамперед мають бути:

– формування правових умов захисту інформації безпосередньо в установах суб'єктів підприємництва. Під такими умовами слід розуміти розробку нормативно-правових документів стосовно захисту всіх видів інформації (документованої, електронної, а також інформації, яка існує у вигляді знань працівників суб'єктів). Зазначеними документами мають регулюватись взаємовідносини суб'єктів підприємництва з їх працівниками, клієнтами, партнерами, кредиторами, контрагентами, іншими особами щодо доступу до інформації суб'єктів, прав щодо її отримання та захисту, відповідальності за неправомірну поведінку стосовно інформації, яка має обмежений доступ;

– створення системи захисту інформації, яка функціонує в інформаційній мережі. Зазначена система має передбачати комплекс організаційних, технічних, апаратних, криптографічних заходів і забезпечувати гарантований захист від посягань на електронну інформацію суб'єктів підприємництва;

– забезпечення контролю за носіями інформації, насамперед працівниками суб'єктів підприємництва, стосовно дотримання ними встановленого режиму захисту інформації, своєчасне реагування на всі збої в захисті інформації, що зберігається та функціонує в інформаційних мережах суб'єктів;

– запровадження надійної системи документообігу в установах суб'єктів підприємництва (службового та спеціального діловодства), яка виключала б можливість несанкціонованого доступу до документів, їх втрати, знищення чи модифікації;

– забезпечення надійної охорони установ суб'єктів підприємництва, особливо з погляду виключення можливості несанкціонованого доступу до їх документів чи електронних носіїв інформації.

Мінімізація ризиків, що виникають під час формування інформаційного ресурсу суб'єкта підприємництва, інформаційного забезпечення його операцій та управлінських рішень, здійснюється через проведення відповідних заходів, передусім інформаційного спрямування. Насамперед звертається увага на організацію інформаційно-аналітичної роботи, яка повинна виконуватись як один з необхідних видів інформаційного забезпечення підприємницької діяльності. Ця робота має передбачати збирання та обробку інформації з різних джерел різними підрозділами суб'єкта підприємництва. На жаль, у більшості суб'єктів цьому питанню не приділяють належної уваги, у кращому разі завдання інформаційно-аналітичної роботи покладають на службу безпеки й цим обмежуються. Тому інформація зазвичай є неповною та односторонньо висвітлює події, явища, об'єкти. Коли ж суб'єкти підприємництва організовують інформаційно-аналітичну роботу як один із елементів їх інформаційного забезпечення, то формування інформаційних ресурсів здійснюється системно по трьох інформаційних рівнях: інформація від

маркетингової діяльності, інформація від проведення інформаційного моніторингу та досліджень контрагентів, клієнтів, партнерів і інформація, отримана від заходів комерційної розвідки.

Крім того, така робота передбачає періодичне проведення в підрозділах суб'єктів підприємництва інформаційного аудиту, під час якого виявляється необхідна для забезпечення конкретної їх діяльності та операцій юридична, комерційна, фінансова, технологічна та інша інформація. Уся інформація, отримана від маркетингової діяльності, інформаційного моніторингу та аудиту, а також комерційної розвідки, узагальнюється, аналізується, за необхідності перевіряється й формується у відповідні бази даних. Тобто основними засадами мінімізації ризиків під час формування інформаційних ресурсів суб'єктів підприємництва є створення ними власної інформаційної бази даних. Якраз зазначена база має стати головним джерелом інформації для інформаційного забезпечення операцій та управлінських рішень в діяльності суб'єктів підприємництва. Водночас така база має постійно оновлюватись і доповнюватись, щоб не допустити її старіння й формування певного ризику її використання.

Для мінімізації інформаційних ризиків впливу суб'єкти підприємництва вдаються до таких заходів:

– періодичне поширення через різні інформаційні канали позитивної інформації про суб'єктів, оприлюднення їх досягнень та активна реклама продукції, послуг, робіт;

– періодичне інформування інформаційного середовища суб'єктів, насамперед персоналу, акціонерів і клієнтів про результати їх роботи;

– формування фірмового патріотизму у персоналу та акціонерів суб'єктів, пропаганда позитивного їх іміджу на ринку;

– проведення спеціальних інформаційних операцій стосовно зміни об'єктів інформаційного впливу, дезорієнтації суб'єктів, що вдаються до заходів впливу, заходів контрпропаганди та антикопроментації.

Мінімізація ризиків інформаційного тероризму здійснюється шляхом проведення заходів захисту технічного, програмного, криптографічного, апаратного, адміністративного, правового характеру власних інформаційних мереж і систем, а також заходів формування стійкого іміджу суб'єктів підприємництва на ринку, пропаганди їх послуг і реклами. Крім того, проводиться низка заходів щодо згуртування колективів працівників суб'єктів підприємництва, формування в них фірмового патріотизму. Важливою частиною заходів мінімізації ризиків інформаційного тероризму є заходи з формування довіри до суб'єктів підприємництва та його менеджменту з боку клієнтів, акціонерів, державних органів.

На мінімізацію ризиків інформаційного тероризму мають бути спрямовані заходи з виявлення та перетинання інформаційних каналів, через які можуть бути здійснені інформаційні атаки.

Крім вищезазначених заходів використовують і інші заходи нівелювання інформаційних ризиків (рис. 8.2).

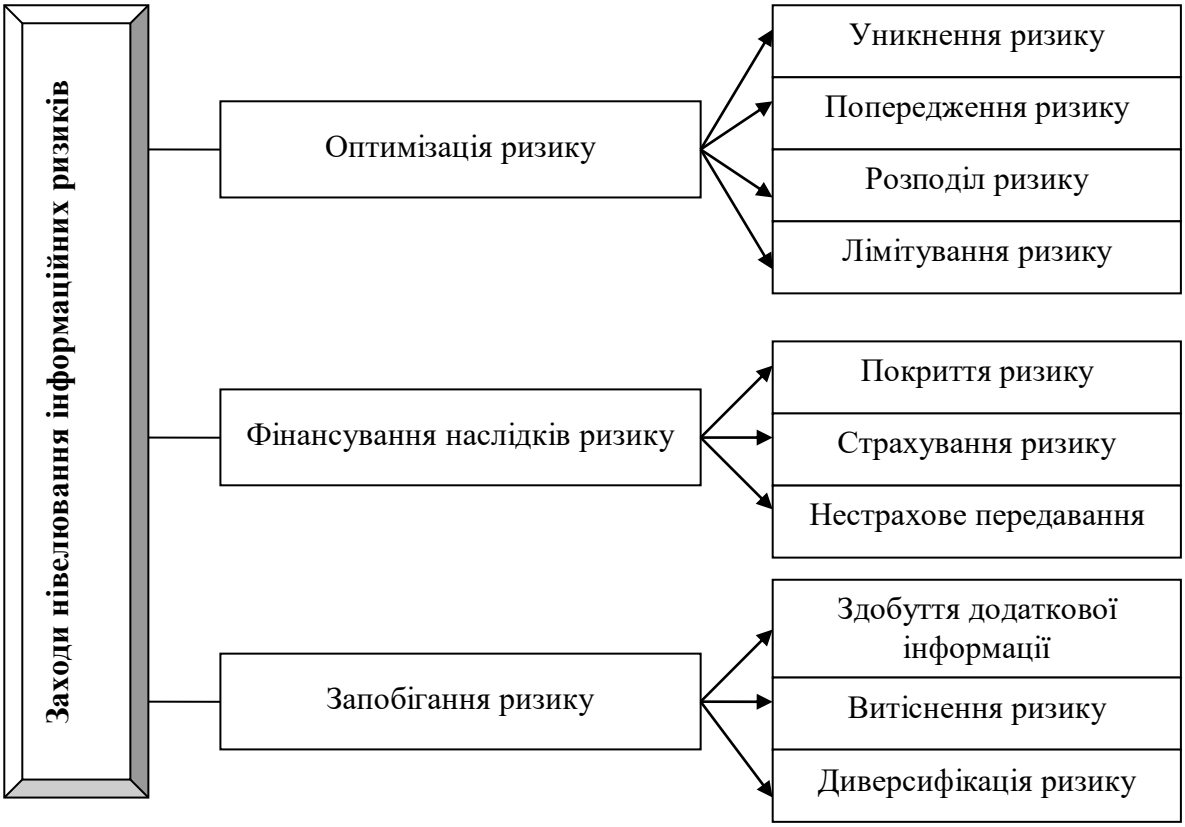

Рис. 8.2. Шляхи нівелювання інформаційних ризиків суб'єкта підприємництва

Оптимізація інформаційного ризику охоплює здійснення таких превентивних заходів: уникнення ризику, попередження ризику, розподіл ризику та лімітування ризику.

Уникнення ризику (ухилення від ризику) – передбачає здійснення процесу захисту інформації в такий спосіб, щоб якнайменше ризиків впливало на нього, або й взагалі відмовитися від певних дій, пов'язаних з ризиком. Уникнення ризику – найпростіший спосіб зниження ризику, в той же час він унеможливлює одержання запланованого результату.

Попередження ризику (запобігання втратам) – здійснення заходів, які сприяють зведенню до мінімуму ймовірність частини втрат. Попередження ризику пов'язане з розробленням і впровадженням програми превентивних заходів, виконання яких слід контролювати і періодично уточнювати з урахуванням змін, що відбулися. Використання цього методу доцільне лише в тому випадку, коли ймовірність реалізації ризику досить велика та прогнозовані витрати на реалізацію превентивних заходів менші, ніж втрати, спричинені ризиком.

Розподіл (дисипація) ризику – залучення до впровадження дій стосовно захисту інформації інших суб'єктів господарювання, кожен із них у випадку невдачі понесе втрати пропорційно до своєї участі та внеску.

Лімітування ризику – встановлення внутрішніх фінансових нормативів (максимальний обсяг товарного кредиту, максимальний період залучення

засобів в дебіторській заборгованості тощо), що будуть враховуватись у процесі захисту інформації.

Фінансування наслідків ризику – забезпечення економічної можливості компенсацій матеріальних збитків, які виникли внаслідок несприятливих випадкових подій (втрати майна, відповідальності за зобов'язання, фінансових втрат, збитків, завданих персоналу, відповідальності за збитки, завдані третім особам тощо). Фінансування наслідків інформаційного ризику передбачає компенсацію ймовірних втрат і збитків у процесі реалізації, використовуючи такі заходи: покриття ризику, страхування ризику, нестрахове передавання ризику.

Покриття ризику – формування грошових резервів на покриття непередбачуваних витрат у процесі захисту інформації. Покриття ризику може бути як запланованим, так і незапланованим. При запланованому покритті ризику вдаються до самострахування, тобто створюють власні резервні фонди усередині самого підприємства – так звані фонди самострахування. При незапланованому покритті ризику втрати покриваються із залишків ресурсів.

Страхування ризику (передавання ризику) – договірне передавання відповідальності за всеможливі ризики в процесі захисту інформації та відшкодування всіх чи частини збитків за рахунок створених страховою організацією грошових фондів. Цей метод нівелювання ризику доречно застосовувати в тому випадку, коли ймовірність реалізації ризику невисока, проте може призвести до значних суттєвих втрат.

Нестрахове передавання ризику – передавання ризику третій особі, тобто передавання діяльності, пов'язаної з ризиком, або фінансової відповідальності за втрати, зумовлені ним.

Запобігання ризику передбачає такі заходи: здобуття додаткової інформації, витіснення ризику, диверсифікацію ризику.

Здобуття додаткової інформації – збільшення витрат ресурсів та часу на отримання додаткової інформації про чинники зовнішнього та внутрішнього середовищ, які пов'язані із захистом інформації, яка дозволяє знизити ризик та зменшити можливі збитки.

Витіснення ризику – виконання дій щодо захисту інформації з одночасним активним впливом підприємства на джерела ризику.

Диверсифікація ризику – розподіл інвестиційних засобів між різними об'єктами вкладення капіталу, що дозволяє мінімізувати можливі втрати.

Отже, використання вищезазначених методів нівелювання інформаційних ризиків залежно від створеної ситуації дасть можливість підприємствам мінімізувати інформаційні ризики та сприятиме досягненню бажаного результату.

ТЕМА 9
КОНЦЕПЦІЯ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

9.1. Специфіка технічного захисту інформації
9.2. Організація і функції підрозділів технічного захисту інформації

9.1. Специфіка технічного захисту інформації

Одним із напрямів захисту інформації в інформаційних системах є технічний захист інформації. Адже на сучасному етапі розвитку суспільства інформація є чи не найдорожчим товаром, одним з найважливіших джерел процвітання будь-якого підприємства. Широкомасштабне впровадження інформаційних технологій потребує значної уваги до питань технічного захисту інформації, оскільки несанкціонований витік її може призвести до втрати підприємством позицій на ринку і значних фінансових збитків.

Питання технічного захисту інформації поділяють на два великих класи завдань:

– захист інформації від несанкціонованого доступу (НСД);
– захист інформації від витоку технічними каналами.

Для розв’язання всього комплексу завдань підприємство повинне співпрацювати з провідними державними та недержавними підприємствами й організаціями, що працюють у сфері захисту інформації, в тому числі: зі Службою безпеки України, державним підприємством «Українські спеціальні системи» та ін.

Захист від НСД може бути здійснений у різних складових інформаційної системи:

– прикладне й системне ПЗ:
– системи розмежування доступу до інформації;
– системи ідентифікації та аутентифікації;
– системи аудиту й моніторингу;
– системи антивірусного захисту.
– апаратна частина серверів та робочих станцій: апаратні ключі; системи сигналізації; засоби блокування пристроїв та інтерфейсів вводу-виводу інформації.
– комунікаційне обладнання і канали зв’язку:

міжмережеві екрани (Firewall) – для блокування атак із зовнішнього середовища:

1) Cisco PIX Firewall;
2) Symantec Enterprise FirewallTM;
3) Contivity Secure Gateway та Alteon Switched Firewall від компанії Nortel Networks. Вони керують проходженням мережевого трафіка відповідно до правил (policies) захисту. Міжмережеві екрани зазвичай установлюють на вході мережі і поділяють на внутрішні (приватні) й зовнішні (загального доступу);

– системи виявлення вторгнень (IDS – Intrusion Detection System) – для виявлення спроб несанкціонованого доступу як ззовні, так і всередині мережі, захисту від атак типу «відмова в обслуговуванні» (Cisco Secure IDS, Intruder Alert та NetProwler від компанії Symantec). Використовуючи спеціальні механізми, системи виявлення вторгнень здатні запобігати шкідливим впливам, що дає змогу значно зменшити час простою внаслідок атаки і витрати на підтримку працездатності мережі;

– засоби створення віртуальних приватних мереж (VPN -Virtual Private Network) – для організації захищених каналів передавання даних через незахищене середовище: Symantec Enterprise VPN; Cisco IOS VPN; Cisco VPN concentrator. Ці віртуальні приватні мережі забезпечують прозоре для користувача сполучення локальних мереж, зберігаючи при цьому конфіденційність та цілісність інформації шляхом її динамічного шифрування;

– засоби аналізу захищеності – для аналізу захищеності корпоративної мережі та виявлення можливих каналів реалізації загроз інформації: Symantec Enterprise Security Manager; Symantec NetRecon. їх застосування дає змогу уникнути можливих атак на корпоративну мережу, оптимізувати витрати на захист інформації та контролювати поточний стан захищеності мережі.

– периметр інформаційної системи, для захисту якого створюються системи: охоронної та пожежної сигналізації; цифрового відеоспостереження; контролю та управління доступом (СКУД).

Захист інформації від її витоку технічними каналами зв'язку забезпечується:

– використанням екранованого кабелю та прокладанням проводів і кабелів в екранованих конструкціях;

– установленням на лініях зв'язку високочастотних фільтрів;

– побудовою екранованих приміщень («капсул»);

– використанням екранованого обладнання;

– установленням активних систем зашумлення;

– створенням контрольованої зони.

Для оцінювання стану технічного захисту інформації, що опрацьовується або циркулює в автоматизованих системах, комп'ютерних мережах, системах зв'язку, та підготовки обґрунтованих висновків для прийняття відповідних рішень проводять експертизу у сфері технічного захисту інформації.

9.2. Організація і функції підрозділів технічного захисту інформації

Інформаційна безпека є комплексом, в якому не можна виділити важливіші чи менш важливі складові, її не можна сприймати інакше, ніж комплекс.

Загрози інформаційній безпеці – чинник або сукупність чинників, що створюють небезпеку функціонуванню й розвитку інформаційного простору, інтересам особистості, суспільства, держави. Основним питанням початкового етапу впровадження системи безпеки є призначення відповідальних осіб за безпеку і розмежування сфер їх впливу. Системні програмісти та адміністратори відносять це завдання до компетенції загальної служби безпеки,

тоді як остання вважає, що цим питанням мають займатися спеціалісти по комп'ютерах.

Вирішуючи питання розподілу відповідальності за безпеку комп'ютерної системи, слід ураховувати такі правила:

– ніхто, крім керівництва, не може прийняти основоположні рішення в галузі політики комп'ютерної безпеки;

– ніхто, крім спеціалістів, не зможе забезпечити правильне функціонування системи безпеки;

– ніяка зовнішня організація чи група спеціалістів життєво не зацікавлені в економічній ефективності заходів безпеки.

Організаційні заходи безпеки інформаційних систем прямо чи опосередковано пов'язані з адміністративним управлінням і належать до рішень і дій, які застосовує керівництво для створення таких умов експлуатації, які зведуть до мінімуму слабкість захисту. Адміністрація здійснює:

– заходи фізичного захисту комп'ютерних систем;

– регламентацію технологічних процесів;

– регламентацію роботи з конфіденційною інформацією;

– регламентацію процедур резервування;

– регламентацію внесення змін;

– регламентацію роботи персоналу й користувачів;

– підбір і підготовку персоналу;

– заходи контролю і спостереження.

Технічний захист інформації (ТЗІ) – діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації.

Технічний захист інформації є важливим чинником реалізації організаційно-правових та інженерно-технічних заходів з метою запобігання витоку інформації за рахунок несанкціонованого доступу до неї, несанкціонованим діям та впливам на інформацію, які призводять до її знищення, порушення цілісності або блокування, а також протидії технічним розвідкам.

Слід дотримуватися заходів захисту в усіх точках мережі, за будь-якої роботи суб'єктів з корпоративною інформацією.

Правову основу технічного захисту інформації в Україні становлять:

– Конституція України;

– закони України;

– міжнародні договори України;

– угоди, обов'язковість виконання яких введена Верховною Радою України;

– укази Президента України;

– постанови Кабінету Міністрів України;

– розпорядження адміністрації Державної служби спеціального зв'язку та захисту інформації України;

– інші нормативно-правові акти з питань технічного захисту інформації.

Підрозділ захисту інформації (ПЗІ) здійснює діяльність відповідно до «Плану захисту інформації», календарних, перспективних та інших планів робіт, затверджених керівництвом компанії. Проте виконання будь-яких завдань структурними підрозділами залежить від суб'єктів системи технічного захисту, якості їхньої підготовки, професіоналізму, матеріального забезпечення і чіткої взаємодії з іншими структурами компанії та органами контролю.

Під суб'єктом у цьому разі розуміють користувача системи, процес, комп'ютер або програмне забезпечення для оброблення інформації. Кожен інформаційний ресурс (комп'ютер користувача, сервер організації або мережеве устаткування) має бути захищений від усіх можливих загроз.

На ПЗІ покладається виконання робіт з:

– визначення вимог щодо захисту інформації в автоматизованій інформаційній системі підприємства (АІС);

– проектування;

– розроблення і модернізації КСЗІ;

– експлуатації;

– обслуговування;

– підтримки працездатності КСЗІ;

– контролю за станом захищеності інформації в комп'ютерних системах (КС).

Для проведення окремих заходів захисту інформації в КС, що пов'язані з напрямом діяльності інших підрозділів компанії, наказом керівництва визначають перелік, строки виконання робіт та виконавців - підрозділи або конкретних осіб. У своїй роботі ПЗІ взаємодіє з підрозділами підприємства (режимно-секретним відділом, службою безпеки, відділом ділової розвідки, службою охорони та ін.), а також з державними органами, установами та організаціями, що займаються питаннями захисту інформації.

У разі потреби до виконання робіт можуть бути залучені зовнішні організації, що мають ліцензії на відповідний вид діяльності у сфері захисту інформації.

У будь-якому каналі зв'язку виникають перешкоди, що призводять до спотворення інформації, яка надходить для опрацювання. Для зменшення вірогідності помилок вживають заходів щодо поліпшення технічних характеристик каналів, використання різних видів модуляції, розширення пропускної спроможності та ін. При цьому також потрібно вживати заходів щодо захисту інформації від помилок або несанкціонованого доступу.

Доступ – це надання можливості використовувати інформацію, що зберігається в ЕОМ (системі).

Будь-яка інформація в машині або системі потребує певного захисту, під яким розуміють сукупність методів управління доступом виконуваних у системі програм до інформації, що зберігається в ній.

Захисту підлягає будь-яка документована інформація, неправомірне поводження з якою може завдати збитку її власникові, користувачеві чи іншій особі.

Завданнями підрозділу захисту інформації є:

1. Забезпечення безпеки інформації структурних підрозділів та персоналу компанії в процесі інформаційної діяльності та взаємодії між собою, а також у взаємовідносинах із зовнішніми вітчизняними та закордонними організаціями.

2. Дослідження технології опрацювання інформації з метою виявлення:

– можливих каналів витоку та інших загроз для безпеки інформації;

– формування моделі загроз; розроблення політики безпеки інформації;

– вивчення заходів щодо її реалізації.

3. Організація та координація робіт, пов'язаних із захистом інформації в компанії, необхідність захисту якої визначається чинним законодавством.

4. Підтримка необхідного рівня захищеності інформації, ресурсів і технологій.

5. Розроблення проектів нормативних і розпорядчих документів, чинних у межах організації, згідно з якими має бути забезпечений захист інформації в компанії.

6. Організація робіт зі створення і використання КСЗІ на всіх етапах життєвого циклу КС.

7. Участь в організації професійної підготовки і підвищенні кваліфікації персоналу та користувачів КС з питань захисту інформації.

8. Формування у персоналу і користувачів компанії розуміння необхідності виконання вимог нормативно-правових актів, нормативних і розпорядчих документів, що стосуються сфери захисту інформації.

9. Організація забезпечення виконання персоналом і користувачами вимог нормативно-правових актів, нормативних і розпорядчих документів із захисту інформації компанії.

10. Проведення контрольних перевірок виконання персоналом і користувачами вимог нормативно-правових актів, нормативних і розпорядчих документів із захисту інформації компанії.

11. Забезпечення визначених політикою безпеки властивостей інформації під час створення та експлуатації КС.

12. Своєчасне виявлення та знешкодження загроз для ресурсів КС, причин і умов порушення її функціонування та розвитку.

13. Створення механізму та умов оперативного реагування на загрози для безпеки інформації, інші прояви негативних тенденцій у функціонуванні КС.

14. Ефективне знешкодження загроз для ресурсів КС або запобігання їм шляхом проведення комплексу правових, морально-етичних, фізичних, організаційних, технічних та інших заходів гарантування безпеки.

15. Керування засобами захисту інформації, керування доступом користувачів до ресурсів КС, контроль за їхньою роботою з боку персоналу ПЗІ, оперативне сповіщення про спроби НСД до ресурсів КС підприємства.

16. Реєстрація, збирання, зберігання, опрацювання даних про всі події в системі, які стосуються безпеки інформації.

17. Створення умов для максимально можливого відшкодування та локалізації збитків, завданих несанкціонованими діями фізичних та юридичних осіб, впливом зовнішнього середовища та іншими чинниками.

18. Зменшення негативного впливу наслідків порушення безпеки на функціонування КС.

Під час створення та експлуатації КСЗІ компанії підрозділ захисту інформації виконує такі функції:

1. Організація процесу керування КСЗІ.

2. Розслідування випадків порушення політики безпеки, небезпечних та непередбачених подій, здійснення аналізу причин, що призвели до них, супроводження банку даних таких подій.

3. Вжиття заходів у разі виявлення спроб НСД до ресурсів КС, порушення правил експлуатації засобів захисту інформації або інших дестабілізаційних факторів.

4. Забезпечення контролю цілісності засобів захисту інформації та швидке реагування на їх вихід із ладу або порушення режимів функціонування.

5. Організація керування доступом до ресурсів КС – розподіл між користувачами необхідних реквізитів захисту інформації:

– паролів;

–привілеїв;

– ключів та ін.

6. Супроводження й активізація бази даних захисту інформації:

– матриці доступу;

– класифікаційні мітки об’єктів;

– ідентифікатори користувачів тощо.

7. Спостереження (реєстрація і аудит подій в КС, моніторинг подій тощо) за функціонуванням КСЗІ та їх компонентів.

8. Підготовка пропозицій щодо удосконалення порядку забезпечення захисту інформації в КС, впровадження нових технологій захисту і модернізації КСЗІ.

9. Організація і проведення заходів з модернізації, тестування, оперативного відновлення функціонування КСЗІ після збоїв, відмов, аварій КС або КСЗІ.

10. Участь у роботах з модернізації КС:

– узгодженні пропозицій щодо введення до складу КС нових компонентів;

– нових функціональних завдань;

– режимів оброблення інформації, заміни засобів оброблення інформації тощо.

11. Забезпечення супроводження й активізації еталонних, архівних і резервних копій програмних компонентів КСЗІ, забезпечення їх зберігання і тестування.

12. Проведення аналітичного оцінювання поточного стану безпеки інформації в КС:

– прогнозування виникнення нових загроз та їх врахування в моделі загроз;

– визначення необхідності її коригування;

– аналіз відповідності технології оброблення інформації;

– аналіз реалізованої політики безпеки поточної моделі загроз та ін.

13. Доведення власникам інформації технічних можливостей захисту інформації в КС і типові правила для персоналу і користувачів КС.

14. Негайне втручання в процес роботи КС у разі виявлення атаки на КСЗІ, проведення у таких випадках робіт з викриття порушника.

15. Регулярне подання звітів керівництву компанії-власника (розпорядника) КС про виконання користувачами КС вимог захисту інформації.

16. Аналіз відомостей про технічні засоби захисту інформації нового покоління.

17. Обґрунтування пропозицій щодо придбання засобів для компанії.

18. Контроль за виконанням персоналом і користувачами КС вимог, норм, правил, інструкцій щодо захисту інформації відповідно до визначеної політики її безпеки.

19. Контроль забезпечення режиму секретності у разі оброблення в КС інформації, що становить державну таємницю.

20. Контроль забезпечення охорони і порядку зберігання документів (носіїв інформації), які містять відомості, що піддягають захисту.

21. Розроблення і реалізація спільно з РСВ компанії комплексних заходів безпеки інформації під час проведення заходів з науково-технічного, економічного, інформаційного співпраці з іноземними фірмами.

22. Розроблення і реалізація спільно з РСВ компанії комплексних заходів безпеки інформації під час проведення нарад, переговорів тощо, здійснення їх технічного та інформаційного забезпечення.

Більшість систем захисту в таких випадках використовують набори привілеїв, тобто для виконання певної функції потрібний певний привілей. Зазвичай користувачі мають мінімальний набір привілеїв, адміністратори - максимальний.

Набори привілеїв охороняються системою захисту. Несанкціоноване (незаконне) захоплення привілеїв можливе за наявності помилок у системі захисту, але здебільшого – в процесі керування системою захисту, зокрема у разі недбалого користування привілеями.

Чітке дотримання правил керування системою захисту, принципу мінімуму привілеїв дає змогу уникнути таких порушень.

Список літератури

1. Господарський кодекс України від 21.10.2004 р. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.
2. Цивільний кодекс України від 16.01.2013 р. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.
3. Закон України «Про доступ до публічної інформації» №2939-VI від 13.01.2011 р. [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua.
4. Закон України «Про захист персональних даних» №2297-VI від 30.09.2015 р. [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua.
5. Закон України «Про інформацію» № 2657-XII від 02.10.1992 р. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua.
6. Богуш В. М. Інформаційна безпека держави : навч. посіб. / В. М. Богуш, О. К. Юдін. – К. : «МК-Прес», 2005. – 432 с.
7. Домарєв В. В. Організація захисту інформації на об’єктах державної та підприємницької діяльності. : навч. посіб. / В. В. Домарєв, С. О. Скворцов. – К. : В-во Європ. ун-ту, 2006. – 102 с.
8. Зубок М. І. Інформаційна безпека в підприємницькій діяльності : підруч. / М. І. Зубок. – К. : ГНОЗІС, 2015. – 216 с.
9. Зубок М. І. Інформаційно-аналітичне забезпечення підприємницької діяльності : навч. посіб. / М. І. Зубок. – К. : КНТЕУ, 2007. – 156 с.
10. Игнатьев В. А. Информационная безопасность современного коммерческого предприятия : монография / В. А. Игнатьев. – Старый Оскол : ООО «ТНТ», 2005. – 448 с.
11. Кузнецов О. О. Захист інформації та економічна безпека підприємства : монографія / О. О. Кузнецов, С. П. Євсеєв, С. В. Кавун. – Х. : ХНЕУ, 2008. – 360 с.
12. Муковський І. Г. Інформаційно-аналітична діяльність в міжнародних відносинах : навч. посіб. / І. Г. Муковський, А. Г. Міщенко, М. М. Шевченко. – К. : Кондор, 2012. – 224 с.
13. Садердинов А. А. Информационная безопасность предприятия : учеб. пособ. / А. А. Садердинов, В. А. Трайнев, А. А. Федулов [2-е изд.]. – М. : «Дашков и К°», 2005. – 336 с.
14. Сідак В. С. Забезпечення інформаційної безпеки в країнах НАТО і ЄС : монографія / В. С. Сідак, В. Ю. Артемов. – К. : КНТ, 2007. – 179 с.
15. Сороківська О. А. Інформаційна безпека підприємства: нові загрози та перспективи / О. А. Сороківська, В. Л. Гевко // Вісник Хмельницького національного університету. – 2010. – № 2. – Т. 2. – С. 32–35.
16. Франчук В. І. Основи економічної безпеки : навч. посіб. / В. І. Франчук. – Львів : «Каменяр», 2008. – 203 с.
17. Щербина В. М. Інформаційне забезпечення економічної безпеки підприємств та установ / В. М. Щербина // Актуальні проблеми економіки. – 2006. – № 10. – С. 220–225.

Основна література для студентів

1. Донець Л. І. Економічна безпека підприємства : навч. посіб. [для студ. вищ. навч. закл.] / Л. І. Донець, Н. В. Ващенко. – К. : Центр уч. л-ри, 2008. – 240 с.
2. Економічна безпека підприємств, організацій та установ : навч. посіб. / [В. Л. Ортинський, І. С. Керницький, З. Б. Живко та ін.]. – К. : Правова єдність, 2009. – 544 с.
3. Живко З. Б. Механізм управління системою економічної безпеки підприємства / З. Б. Живко // Науковий вісник Ужгород. ун-ту. Серія «Економіка». – 2014. – Вип. 3 (44). – С. 37–42.
4. Заїнчковський А. О. Економічна безпека підприємства : навч. посіб. [для студ. вищ. навч. закл.] / А. О. Заїнчковський, Т. М. Іванюта. – К. : Центр уч. л-ри, 2009. – 256 с.
5. Зубок М. І. Інформаційна безпека : навч. посіб. / М. І. Зубок. – К. : КНТЕУ, 2005. – 133 с.
6. Кормич Б. А. Інформаційна безпека: організаційно-правові основи : навч. посіб. / Б. А. Кормич. – К. : Кондор, 2004. – 384 с.
7. Крегул Ю. І. Комерційна розвідка та внутрішня безпека на підприємстві / Ю. І. Крегул, М. І. Зубок, Р. О. Банк. – К. : КНТЕУ, 2014. – 176 с.
8. Кузнецов О. О. Захист інформації та економічна безпека підприємства : монографія / О. О. Кузнецов, С. П. Євсеєв, С. В. Кавун. – Харків : ХНЕУ, 2008. – 360 с.

Додаткова література для студентів

1. Долженков О. Ф. Особливості гарантування економічної безпеки підприємницької діяльності в ринкових умовах : монографія / О. Ф. Долженков, Ж. О. Жуковська, О. М. Головченко. – Одеса : ОЮІ ХНУВС, 2007. – 208 с.
2. Зацеркляний М. М. Основи економічної безпеки : навч. посіб. / М. М. Зацеркляний, О. Ф. Мельников. – К. : КНТ, 2009. – 337 с.
3. Камлик М. І. Економічна безпека підприємницької діяльності. Економіко-правовий аспект : навч. посіб. / М. І. Камлик – К. : Атіка, 2005. – 432 с.
4. Коженьовскі Л. Управління безпекою / Л. Коженьовскі // Актуальні проблеми економіки. – 2004. – №1 (31). – С. 147–154.
5. Козаченко А. В. Экономическая безопасность предприятия: сущность и механизм обеспечения : монография / А. В. Козаченко, В. П. Пономарев, А. Н. Ляшенко. – К. : Либра, 2003. – 280 с.
6. Куркін М. В. Контроль та захист економічної безпеки діяльності підприємств : навч. посіб. / М. В. Куркін, В. Д. Понікаров, Д. В. Назаренко. – Х. ; ФОП Павленко О. Г.; ВД «ІНЖЕК», 2010. – 300 с.
7. Моделювання економічної безпеки: держава, регіон, підприємство : монографія / [Геєць В. М., Кизим М. О., Клебанова Т. С., Черняк О. І. та ін.] ; за ред. Гейця В. М. – Х. : ВД “ІНЖЕК”, 2006. – 240 с.

8. Мойсеєнко І. П. Управління фінансово-економічною безпекою підприємства : навч. посіб. / І. П. Мойсеєнко, О. М. Марченко. – Львів : ЛДУВС, 2011. – 380 с.
9. Основи економічної безпеки : [підруч.] / О. М. Бандурка, В. Є. Духов, К. Я. Петрова, І. М. Червяков. – Київ : Вид-во нац. ун-ту внутр. справ, 2003. – 236 с.
10. Основы экономической безопасности (Государство, регион, предприятие, личность) / [под ред. Е. А. Олейникова]. – М. : ЗАО «Бизнес-школа «Интел-Синтез», 1997. – 288 с.
11. Франчук В. І. Основи економічної безпеки : навч. посіб. / Франчук В. І. – Львів : «Каменяр», 2008. – 203 с.

Навчальне видання

Укладачі
Мохнюк Анна Миколаївна
Скорук Олена Володимирівна

Організація та управління інформаційною безпекою на підприємстві

Конспект лекцій

Друкується в авторській редакції