Лекція 8-9

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ ПІДПРИЄМСТВА

1. Система захисту інформації суб'єкта господарської діяльності: поняття, значення, принципи.
2. Організаційні заходи для створення системи захисту інформації суб'єкта господарювання.
3. Зміст завдань системи захисту інформації.
4. Напрями роботи персоналу з питань захисту інформації підприємства
5. Організації системи діловодства щодо інформаційних матеріалів таємного та конфіденційного характеру

1. Система захисту інформації суб'єкта господарської діяльності: поняття, значення, принципи

З інформаційної точки зору суб'єкт господарської діяльності являє собою комплекс компонентів, пов'язаних між собою єдиною метою, структурними відносинами, технологіями інформаційного обміну. Зазначені компоненти в процесі функціонування суб'єкта можуть змінюватись, на них можуть здійснювати вплив різного роду внутрішні та зовнішні чинники, які складно прогнозувати та оцінювати. Всі компоненти можна сформувати у чотири групи: персонал, технічні засоби інформатизації, програмне забезпечення, документи і вважати як об'єкти захисту інформації. Зазначені групи у своєму функціонуванні зазнають впливу різного роду специфічних факторів і, взаємодіючи між собою, впливають один на одного, формуючи відповідний стан інформаційної безпеки суб'єкта підприємництва. Як показує практика, робота з кожною з цих груп щодо забезпечення інформаційної безпеки чи зокрема захисту інформації призводить до покращення якостей безпеки по одних параметрах і погіршення по інших, що вимагає комплексного підходу до забезпечення інформаційної безпеки[1].

Висока інформатизація та автоматизація виробничого процесу суб'єктів господарювання не виключає звичайних взаємовідносин їх персоналу з контрагентами та клієнтами, а значні обсяги електронних документів аж ніяк не призводять до зменшення документообігу паперових носіїв інформації. Тобто забезпечення інформаційної безпеки і такої її складової як захист інформації неможливо здійснити лише організаційними

[1] Зубок М. І. Інформаційно-аналітичне забезпечення підприємницької діяльності. К.: ГНОЗІС, 2015. 216 с.

чи технічними заходами, або скажімо програмними чи криптографічними. Дії по забезпеченню інформаційної безпеки повинні являти собою регулярний процес, що здійснюється на всіх напрямках діяльності суб'єкта підприємництва на основі комплексного застосування всіх заходів і засобів безпеки. При цьому засоби, заходи та методи безпеки найбільш раціональним способом об'єднуються в єдиний цілісний механізм не тільки для захисту від зловмисників, але і від некомпетентних, недобросовісних працівників та різних непередбачуваних ситуацій. Тобто, забезпечення інформаційної безпеки як має носити системний та комплексний характер. Системність заходів інформаційної безпеки суб'єктів господарської діяльності має передбачати наступне:

- високий ступінь захищеності їх інформації як головну характеристику її якісного стану;
- заходами безпеки охоплюються всі інформаційні ресурси суб'єктів підприємництва;
- діяльність по забезпеченню 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. Крім того, значний спектр різного роду операцій, велика регіональна розпорошеність установ, специфічність поведінки персоналу, контрагентів, суб'єктів господарської діяльності та клієнтів створюють суттєві особливості їх діяльності і вимагають адекватної реакції систем безпеки. Водночас адекватність реакції передбачає узгоджені дії всіх сил та засобів безпеки, що можливо лише при системному підході. Більш того, забезпечення безпеки в сучасних умовах має здійснюватися як на технологічному, так і на логічному рівнях, що має забезпечувати врахування всіх факторів і особливостей, які впливають на безпеку суб'єктів підприємництва, а також всіх компонентів інформаційної роботи: збору, обробки, зберігання, передавання, використання інформації. За таких умов системність та комплексність інформаційної безпеки, в тому числі і у сфері захисту інформації є обов'язковою умовою її високої ефективності.

Система захисту інформації суб'єкта господарської діяльності — 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 суб'єктів підприємництва.

Враховуючи складність структури системи захисту інформації та необхідність її функціонування в умовах невизначеності, побудова такої системи має базуватись на відповідних принципах.

Принцип повноти інформації, що захищається обумовлює необхідність захисту не тільки інформації з обмеженим доступом, а і іншої інформації, втрата якої може нанести шкоди суб'єкту господарської діяльності. Реалізація даного принципу дозволяє забезпечувати захист всіх об'єктів інтелектуальної власності суб'єкта господарської діяльності.

Відповідно до принципу обґрунтованості захисту інформації визначається доцільність надання відповідного грифу певним відомостям, виявляються економічні та інші наслідки, що можуть наступати від застосування заходів захисту інформації. Це в свою чергу дозволить більш раціонально та продуктивно здійснювати витрати на захист інформації.

Принципи повної участі та персональної відповідальності передбачають поширення обов'язку захищати інформацію на всіх осіб, що працюють з інформаційними продуктами (програмами, документами, характеристиками) суб'єкта господарської діяльності, а також вимагають відповідальності кожного із його працівників чи інших осіб за порушення заходів захисту інформації.

Принцип превентивності передбачає плановість заходів захисту інформації, застосування їх з метою виявлення, перетинання та локалізації загроз інформації суб'єкта господарської діяльності.

2. Організаційні заходи для створення системи захисту інформації суб'єкта господарювання

Важливе значення у захисті інформації має політика інформаційної безпеки суб'єкта господарської діяльності. ***Політика інформаційної безпеки*** — це прийнята у суб'єкта господарської діяльності сукупність норм, правил, рекомендацій згідно яких будується система його інформаційної безпеки та управління нею. Вона реалізується за допомогою організаційних заходів і

програмно-технічних засобів, які визначають архітектуру системи захисту та за допомогою засобів управління механізмами захисту. Для кожного суб'єкта господарської діяльності політика безпеки є індивідуальною і залежить від особливостей технологій його виробничої та комерційної діяльності, його відносин та умов функціонування на ринку.

Відповідно до прийнятої політики інформаційної безпеки проводяться організаційні заходи по створенню системи захисту інформації. В даний час суб'єктами господарської діяльності напрацьовано відповідний **алгоритм роботи** по організації системи захисту інформації, який включає наступні дії:

- визначення вразливості інформації суб'єкта господарської діяльності (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 господарської діяльності;
- 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. Зміст роботи по визначенню вразливості інформації показано в таблиці 1.

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.

За деякою практикою суб'єкти господарської діяльності не передбачають захисту відкритої інформації. Але ж відкритість інформації не лишає її цінності, а цінна інформація безумовно має захищатись, насамперед від втрати її. Захист такої інформації здійснюється шляхом реєстрації її носіїв, обліку, контролю наявності. Разом з тим, захист відкритої інформації не повинен обмежувати її загальнодоступності, але доступ до неї має бути контрольованим, з дотриманням відповідних вимог щодо її збереження. Тобто, відкрита інформація є об'єктом захисту і стосовно неї повинні проводитись певні заходи в системі захисту інформації. Загальною ж основою для вибору об'єкту захисту є цінність інформації

Таблиця 1 - Визначення уразливості інформації з обмеженим доступом в діяльності суб'єкта підприємництва

Аналіз цінності інформації	**Аналіз захищеності інформації**	**Аналіз політики захисту інформації**
- актуальність інформації на даний час; - роль конкретної інформації у певній операції або планах розвитку суб'єкта підприємництва; - зацікавленість у подібній інформації інших суб'єктів; - наслідки втрати інформації	– можливості технічних та програмних засобів, що використовуються для захисту інформації, їх стійкість; - категорія інформації (конфіденційна, таємна); - вид інформації (знання, документи, електронна інформація); - характеристика місць зберігання носіїв інформації, можливість доступу до них; - можливість зміни або знищення інформації	– організація захисту інформації в діяльності суб'єкта підприємництва; - ефективність заходів захисту інформації; - характеристика поведінки персоналу щодо збереження інформації; - стан забезпечення системи захисту інформації
Чи є інформація цінною для осіб заці-кавлених у її отриманні	*Вірогідність несанкціонованого доступу до носіїв інформації*	*Можливість витоку інформації за ініціа-тивою працівників*
Висновок	**Висновок**	**Висновок**

Критеріями цінності можуть бути: необхідність інформації для правового забезпечення діяльності суб'єкта підприємництва; необхідність інформації для здійснення виробничої діяльності; необхідність інформації для ефективного управління діяльністю суб'єкта підприємництва, об'єктивного прийняття управлінських рішень, організації прибуткової його діяльності; необхідність

інформації для формування ресурсної бази суб'єкта підприємництва та забезпечення його безпеки.

Разом з тим основним і визначальним критерієм у виборі об'єкта захисту інформації є можливість отримання від використання певної інформації переваг за рахунок її невідомості третім особам. Критерій має дві складові: невідомість інформації для третіх осіб і отримання вигоди в силу цієї невідомості.

3. Зміст завдань системи захисту інформації

Водночас система захисту інформації суб'єкта господарської діяльності у своєму функціонуванні носить конкретний характер і вимагає однозначної конкретизації об'єктів захисту. Інформація, на яку спрямовуються зусилля системи захисту не існує сама по собі, а фіксується (відображається) у відповідних матеріальних об'єктах або пам'яті людей, тобто вона існує на відповідних носіях. Таким чином, обираючи об'єкт захисту ми маємо визначити певний перелік носіїв невідомої третім особам інформації, за рахунок якої суб'єкт отримує певні переваги у своїй діяльності. Тобто, це можуть бути відповідні документи, матеріали (в тому числі магнітні, магнітооптичні, оптичні та інші засоби), вироби (засоби відображення, обробки, відновлення, передачі інформації), мережі зв'язку та передачі даних, а також працівники суб'єкта. Захист цих об'єктів має здійснюватися шляхом регулювання доступу до них, встановлення відповідного порядку їх використання (діяльності) та формування умов зберігання. Якраз ці заходи і складають структуру системи захисту інформації.

Зазначені заходи в системі захисту інформації здійснюється за допомогою технічних, програмних та організаційно-правових засобів. До технічних засобів регулювання доступу можна віднести кодовані замки на вході в приміщення де знаходиться відповідна інформація, встановлення засобів та систем пропуску на територію суб'єкта підприємництва, спеціальні прилади та пристрої, що регулюють доступ до інформації, яка зберігається у комп'ютерах. За допомогою програмних засобів розмежовується доступ до інформації в інформаційних комп'ютерних системах і мережах. Правові засоби є загальними, які встановлюють як порядок роботи з інформаційними ресурсами суб'єкта підприємництва, так і умови та правила використання технічних та програмних засобів захисту інформації.

Враховуючи різноманітність загроз інформації суб'єктів господарської діяльності та необхідність найбільш ефективного її захисту,

система має виконувати відповідний комплекс завдань орієнтований на використання всіх можливих засобів.

Таблиця 2 – Зміст завдань системи захисту інформації

Завдання	
Правового характеру	• регулювання доступу до інформаційних ресурсів суб'єкта підприємництва представників державних органів і установ; • регулювання доступу персоналу до інформаційних ресурсів суб'єкта підприємництва; • встановлення відповідальності за посягання на інформаційні ресурси суб'єкта підприємництва
Криптографічного характеру	• шифрування інформації при передачі її через незахищені засоби зв'язку; • регламентація доступу до баз даних та електронних документів
Організаційного характеру	• категоріювання інформації суб'єкта підприємництва • встановлення відповідного режиму роботи суб'єкта підприємництва; • організація спеціального діловодства в діяльності суб'єкта підприємництва; • 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 і т. і.; • планування дій щодо захисту інформації при стихійних лихах, пожежах, терористичних актах, інших негараздах.
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
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

4. Напрями роботи персоналу з питань захисту інформації підприємства

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

У цьому сенсі працівники суб'єктів господарської діяльності 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.

Заборони та обмеження досягаються виключенням фізичної та іншої можливості доступу до інформації, яка згідно повноважень працівника йому не повинна доводитись. Крім того, обмеження доступу здійснюється і шляхом

виконання певних завдань чи робіт по окремих частках групою працівників, кожен з якої не обізнаний із змістом інформації, яка повністю характеризує завдання (обсяг роботи).

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 та ін.

Важливе значення мають заходи протидії попадання працівників під вплив осіб, зацікавлених в отриманні інформації суб'єктів господарської діяльності (конкурентів, промислових шпигунів). Як правило, підрозділи безпеки суб'єктів господарської діяльності розробляють відповідні методики роботи з персоналом щодо протидії витоку інформації, якою володіють працівники. Зазвичай до змісту таких методик включаються наступні питання: визначення готовності кандидатів на роботу та працівників до зрадництва, легкої наживи, аморальної поведінки; формування сприятливих умов роботи кожному із працівників; формування умов та можливостей максимального заробітку та кар'єри; вжиття заходів гарантованого захисту інформаційних об'єктів та регламентування доступу до джерел інформації; встановлення відповідальності за посягання на інформацію суб'єктів підприємництва; пропаганда захисту таємниць суб'єктів підприємництва як однієї із умов ефективного їх розвитку та забезпечення добробуту працівників, вжиття заходів з профілактики недобросовісної їх поведінки; контроль роботи, поведінки та зв'язків працівників, обізнаних з таємницями суб'єктів підприємництва; встановлення в діяльності суб'єктів підприємництва суворого пропускного режиму; контроль наявності документів, стану документообігу, в тому числі і в комп'ютерних мережах, переговорів через засоби зв'язку; аналіз можливих способів посягання на інформацію суб'єктів підприємництва та методів протидії їм з практики роботи інших суб'єктів.

З питань захисту інформації працівники суб'єктів господарської діяльності зобов'язані:

- зберігати в таємниці всі службові відомості, з якими вони ознайомлені у зв'язку зі своєю роботою на посаді;
- виконувати встановлений порядок і правила роботи з документами та інформацією, які мають таємний або конфіденційний характер;
- знати кому із працівників і в якому обсязі дозволено працювати з ві-

домостями обмеженого доступу;

- на вимогу працівників підрозділу безпеки надавати документи, матеріали, електронні носії інформації для перевірки;
- не користуватись на робочому місці власними засобами зберігання та передачі інформації, фото- та відеоапаратурою;
- дотримуватись встановлених правил передачі (пересилання, обробки) інформації з службових документів, ведення службових переговорів, в тому числі і по засобах зв'язку;
- негайно доповідати безпосередньому керівнику про втрату документів службового призначення, особливо тих, що мають гриф таємності;
- своєчасно інформувати підрозділи безпеки про спроби сторонніх осіб отримати інформацію таємного чи конфіденційного характеру.

Захист інтересів суб'єктів господарської діяльності у взаємовідносинах з персоналом, допущеним до їх таємниць здійснюється шляхом правового закріплення таких взаємовідносин у відповідних документах.

- **Зобов'язання про нерозголошення інформації з обмеженим доступом**

Правовий документ, в якому працівник добровільно письмово дає згоду на обмеження його прав щодо використання інформації суб'єкта підприємництва з обмеженим доступом.

Одночасно працівник попереджується про відповідальність за розголошення такої інформації

- **Трудовий договір (контракт*). Наявність у договорі:***

– зобов'язань працівника не розголошувати відомості, які становлять таємну або конфіденційну інформацію;
– зобов'язань працівника дотримуватись правил захисту інформації з обмеженим доступом визначених суб'єктом підприємництва
– зобов'язань працівника повідомляти безпосереднього керівника і службу безпеки суб'єкта підприємництва про втрату носіїв інформації з обмеженим доступом;
– видів відповідальності працівника за недотримання ним правил захисту інформації

- **Наказ про призначення на посаду**

– визначається ступінь допуску до відомостей, які становлять таємну та конфіденційну інформацію;
– визначаються обов'язки працівника та заходи, які повинні ним вживатись для захисту інформації

- **Посадова інструкція**

– обов’язок працівника дотримувати у таємниці відомості, які йому стали відомі у зв’язку з його роботою у суб’єкта господарювання
– відповідальність працівника за порушення правил зберігання інформації суб’єкта господарювання

При звільненні працівників з роботи захист інформації здійснюється шляхом виконання таких заходів:

– отримання від працівників, які звільняються всіх матеріалів конфіденційного та таємного характеру, що обліковуються за ними з оформленням відповідного акту;

– передача працівниками, що звільняються, перепусток, печаток, штампів, ключів, сейфів тощо уповноваженим від суб’єкта підприємництва особам;

– проведення бесіди з працівниками, які звільняються з роботи, про необхідність збереження в таємниці всіх відомостей таємного та конфіденційного характеру, які були їм відомі під час роботи, підписання зобов’язань про нерозголошення ними цих відомостей;

– попередження працівників про відповідальність за розголошення чи використання таємних або конфіденційних відомостей, що належать суб’єкту підприємництва. Підписані працівниками зобов’язання зберігаються в їх особових справах протягом всього терміну зберігання справ.

Практика забезпечення безпеки діяльності суб’єктів господарювання знає приклади коли витік цінної для них інформації здійснювався мимовільно, без злого наміру, в силу недоопрацювання певних питань чи не врахування особливостей ситуації, яка склалась навколо них. Система захисту інформації у зв’язку з цим має поширювати свій вплив і на такі випадки, зокрема щодо пропагандистських, рекламних заходів, публікації звітів, проспектів емісії акцій, оголошень та інших заходів, які проводяться суб’єктами підприємництва, оприлюдненням певної інформації в інформаційному середовищі. Тут інформація має надаватись у так званому диверсифікованому вигляді. Диверсифікація в даному випадку передбачає надання інформації по різних інформаційних каналах, через різних суб’єктів, окремими частками, з перервою у часі.

Чинне законодавство передбачає право доступу до інформації суб’єктів підприємництва представникам державних органів. Тут інформація подається за рішенням керівника установи суб’єкта господарювання в межах

повноважень, якими наділений зазначений представник та в порядку, який встановлений суб'єктом.

Однією з особливостей сьогодення є поширене використання різноманітних електронних засобів для отримання інформації з акустичного каналу. За таких умов система захисту інформації суб'єктів підприємництва має передбачати нормативне регулювання питань, пов'язаних з правилами користування технічними засобами накопичення, обробки, зберігання та передачі інформації. Крім того, доцільним є включити в перелік заходів захисту інформації періодичне проведення атестації окремих приміщень установ суб'єктів підприємництва на предмет наявності в них пристроїв електронної розвідки. До заходів протидії витоку інформації через спеціальні електронні пристрої слід включити спеціальне інженерно-технічне обладнання приміщення де зберігається, оброблюється інформація з обмеженим доступом та обговорюються важливі для суб'єкта підприємництва питання. Сюди ж слід додати і використання спеціальних технічних засобів виявлення пристроїв електронної розвідки та періодичний огляд засобів і мереж зв'язку, місць їх розташування. Звичайно, що система захисту інформації повинна забезпечувати технічний захист інформації, яка оприлюднюється у ході переговорів, нарад та інших видів конфіденційного спілкування.

5. Організація системи діловодства щодо інформаційних матеріалів таємного та конфіденційного характеру

У захисті інформації суб'єктів господарювання 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. Водночас у ході руху документів конфіденційного та таємного характеру збільшується кількість осіб, обізнаних з цінною інформацією, а з тим і розширюються потенційні можливості втрати конфіденційної та таємної інформації, збільшується ризик розголошення її персоналом, витоку через технічні засоби, зникнення документів. У такому

випадку документообіг, як процес руху документованої інформації з обмеженим доступом, також стає об'єктом захисту. Головним у конфіденційному документообігу стає формування спеціальної технології руху документів, яка б забезпечувала необхідну безпеку інформації на будь-якому із етапів її обігу. Тому захищений документообіг має являти собою контролюючий рух документів конфіденційного та таємного характеру по регламентованих пунктах приймання, обробки, розгляду, виконання, використання, зберігання в жорстких умовах організаційного і технологічного забезпечення безпеки як носіїв інформації, так і її самої. У такому разі в доповнення до правил службового документообігу конфіденційний документообіг додатково включає наступні заходи:

- обмеження доступу персоналу до документів справ і баз даних діловою, службовою та виробничою необхідністю;
- персональна відповідальність посадових осіб за надання дозволу на доступ працівників суб'єктів підприємництва до відомостей і документів конфіденційного і таємного характеру;
- жорстка регламентація порядку роботи з документами, справами, базами даних для всього персоналу.

Документообіг, як головна складова діловодства, базується на відповідній систематизації документів якою є номенклатура справ. Згідно з номенклатурою справ всі документи групуються у відповідні групи (справи) і обліковуються та зберігаються по таких групах (справах). Номенклатура справ є єдиною для установи суб'єкта підприємництва. Документообіг здійснюється у відповідності з номенклатурою справ та поділяється на вхідний, вихідний та внутрішній документопотоки. Вхідний документопотік спеціального діловодства включає: приймання, облік і первинну обробку пакетів, конвертів та незаконвертованих документів, що надійшли до установи суб'єкта підприємництва; облік документів і формування довідково-інформаційного банку даних по документах; попередній розгляд і розподіл документів; розгляд документів керівниками і надання їх на ознайомлення з документами виконавців, використання чи виконання.

Вихідний та внутрішній документопотоки включають: вироблення документів (визначення грифу таємності та облік носія майбутнього документу, розробка документу, облік підготовленого документу та його виготовлення; контроль процесу вироблення документів); обробка виданих документів: експедиційна обробка і відправлення їх адресатам, передавання внутрішніх документів відповідним підрозділами суб'єкта підприємництва; систематизація вироблених документів відповідно до номенклатури справ,

оформлення їх по справах; підготовка і направлення справ до архіву суб'єкта підприємництва відповідно з встановленим порядком архівації документів. Всі документи, справи і носії інформації повинні мати інвентарний номер.

Спеціальне діловодство є централізованим і забезпечується відповідним підрозділом. Основною особливістю документообігу в спеціальному діловодстві є багатоступеневий облік всіх процедур і операцій, що проводяться з документами.

Важливе місце в організації захисту інформації в діяльності суб'єктів господарювання є визначення режиму функціонування інформації. Режим, як правило, обирається у залежності від категорії інформації, її цінності для діяльності суб'єкта та зацікавленості в ній інших осіб. Тут можна пропонувати три режими: повністю закритий режим функціонування інформації, частково закритий режим та періодично закритий режим. У першому випадку доступ до інформації надається виключно обмеженому колу осіб і практично ніколи така інформація не розкривається у зв'язку з втратою цінності та її категорії. Документи, в яких міститься подібна інформація з втратою їх значення, як правило, знищується. Частково закритий режим функціонування інформації встановлюється шляхом надання доступу до окремих відомостей певному колу осіб при неможливості їх спілкування між собою з метою узагальнення отриманих відомостей. Періодично закритий режим інформації встановлюється для інформації, яка характеризує нові розробки, види продукції, тривалі відносини або види діяльності, що пов'язані з розвитком бізнесу (проникнення в нові регіон, сегменти ринку, сфери діяльності та ін.).

В умовах режимного функціонування можуть застосовуватись різні способи захисту інформації, які поділяються на активні, пов'язані з протидією загрозам та пасивні – спрямовані на захист від загроз. Активними можна вважати періодичну атестацію приміщень, в яких зосереджена цінна для суб'єктів підприємництва інформація або проводиться робота з нею, а також періодичне обстеження засобів обробки і передачі інформації. Сюди ж доцільно віднести періодичні перевірки наявності документів та вимірювання електромагнітних випромінювань і наводок. Обов'язковим має бути встановлення контролю персоналу, допущеного до роботи з інформацією обмеженого доступу суб'єктів підприємництва.

У окремих випадках, з метою протидії посяганням на інформацію суб'єктів підприємництва, останні можуть вдаватись до дезінформації осіб, які генерують такі загрози щодо місць знаходження інформації, її важливості, провокувати їх на дії через які вони будуть компрометувати себе.

Серед способів захисту інформації може бути її нормування, розмежування доступу до різної за цінністю інформації, поставлення акустичних, електромагнітних та технічних завад, запровадження пропускного режиму, спеціальна охорона місць зберігання інформації і т. д.

Важливу роль у забезпеченні ефективного функціонування системи захисту інформації в діяльності суб'єктів господарювання відіграє правильне управління такою системою, яка має здійснюватися 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 здійснюватися 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.

🕮 Список рекомендованої літератури

1. Конституція України. Закон України від 28 червня 1996 р. *Відомості Верховної Ради України.* 1996. №30. Ст. 141.
2. Господарський кодекс України: Закон України від 16 січня 2003 р. № 436-IV. *Відомості Верховної Ради України*. 2003. №№ 18, 19–20, 21–22. Ст. 144.
3. Цивільний кодекс України від 16 січня 2003 р. № 435-IV. Відомості *Верховної Ради України.* 2003. № 40-44. Ст.356.
4. Про інформацію: Закон України від 2 жовтня 1992 р. *Відомості Верховної Ради України.* 1992. № 48. Ст. 650.
5. Зубок М. І. Інформаційно-аналітичне забезпечення підприємницької діяльності. К.: ГНОЗІС, 2015. 216 с.
6. Кормич Б. А. Інформаційне право. Підручник. Харків: БУРУН і К., 2011. 334 с.
7. Крегул Ю.І., Зубок М.І. Правове регулювання безпеки підприємницької діяльності: навч. посібник. К.: КНТЕУ, 2013. 216с.