Лекція 5

ОСНОВИ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

1. Інформаційна безпека підприємства: поняття, структура
2. Мета, завдання та принципи організації інформаційної безпеки підприємств
3. Процес організації інформаційної безпеки підприємства: поняття, структура.

1.Інформаційна безпека підприємства: поняття, структура

Сучасні особливості інформаційного розвитку суттєво відбились на всі сфери суспільного життя в т. ч. і на підприємницькій діяльності. Формування, в результаті такого розвитку, інформаційних відносин є постійним атрибутом не лише діяльності, а і взагалі існування суспільства, громади, організацій, суб'єктів економічної діяльності. Така ситуація зумовила як певний прогрес, так і створила передумови до появи нового виду ризиків, небезпек та загроз – інформаційних. У процесі взаємовідносин суб'єктів підприємництва інтенсивність інформаційних ризиків, небезпек та загроз характеризується якістю самих взаємовідносин. Якщо в умовах інформаційного співробітництва та взаємодії можливість їх виникнення є мінімальною, то у інших видах взаємовідносин підстави виникнення інформаційних ризиків, небезпек та загроз будуть суттєво зростати. У такому випадку суб'єкти підприємництва мають бути готовими вживати адекватні заходи захисту та протидії таким ризикам, небезпекам та загрозам. Безумовно, що захист та протидія зазначеним небезпекам та загрозам, мінімізація інформаційних ризиків в діяльності суб'єктів підприємництва мають формувати окремий напрямок забезпечення їх безпеки – інформаційну безпеку.

Дослідження, проведені автором у сфері інформаційної безпеки підприємницької діяльності, показали, що сучасні уявлення про безпеку бізнесу взагалі і інформаційну зокрема є досить різноманітними, єдине бачення суті та змісту інформаційної безпеки відсутнє. Не вдаючись до детального аналізу точок зору різних авторів щодо розуміння інформаційної безпеки підприємництва, можна бачити наявність в них певних засад, якими автори ідентифікують інформаційну безпеку. Такими засадами виступає захист інформації. Якраз захист інформації є притаманним позиції переважної більшості авторів у їх розумінні суті інформаційної безпеки. Віддаючи належне таким міркуванням слід звернути увагу на багатофункціональність інформації, яка проявляється у підприємницькій діяльності. Як уже говорилося вище,

інформація є основою знань, тобто інтелектуального потенціалу суб'єктів підприємництва і які безумовно необхідно захищати. В той же час інформація є умовою 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. Тобто, відтотоження інформаційної безпеки лише з захистом інформації при такій різноманітності її властивостей і функцій буде мабуть не логічним. За думкою автора, інформаційна безпека, крім захисту інформації (інформаційного ресурсу суб'єкта підприємництва), має бути спрямована на мінімізацію інформаційного ризику, ще має вирішальне значення для управління господарюючими суб'єктами та забезпечення їх розвитку. Враховуючи, ще інформаційні технології можуть являти собою вид інтелектуальної зброї і негативно впливати на підприємницьку діяльність окремих суб'єктів. Інформаційна безпека має включати в себе функції з протидії інформаційно-психологічному впливу, використанню технологій маніпулювання індивідуальною та колективною свідомістю. При тому підході ***інформаційну безпеку підприємницької діяльності*** *можна розуміти, як стан інформаційної роботи суб'єктів підприємництва за якого забезпечується ефективне інформаційне супроводження їх діяльності, надійний захист інформаційного ресурсу та результативна протидія негативному інформаційно-психологічному впливу на них.*

Тобто, структуру інформаційної безпеки суб'єкта підприємництва складають три складові, наведені на рис. 1. Враховуючи динамічний характер сучасного інформаційного простору, такий підхід до розуміння суті та змісту інформаційної безпеки забезпечує суб'єктам підприємництва 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 суб'єктів підприємництва у інформаційному середовищі.

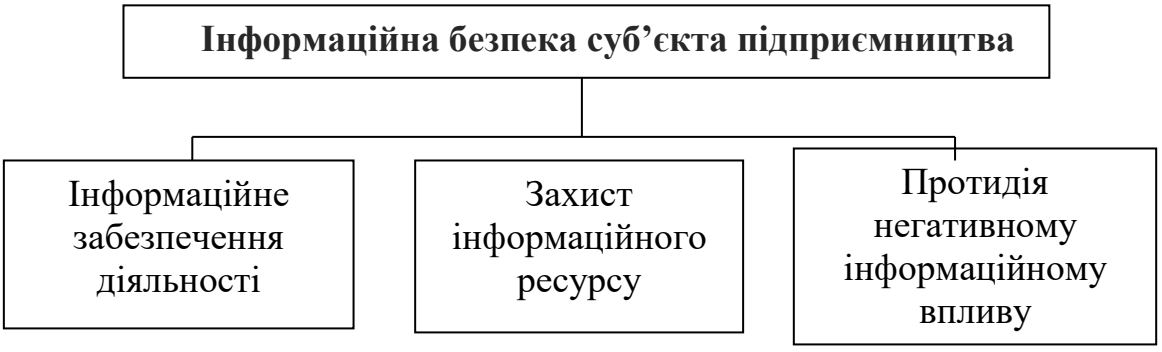

Рис. 1. Структура інформаційної безпеки підприємства

2. Мета, завдання та принципи організації інформаційної безпеки підприємств

Метою інформаційної безпеки у такому випадку є виключення можливості втрати суб'єктами підприємництва 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*, серед яких:

- організація відповідного режиму функціонування інформації в діяльності суб'єктів підприємництва;
- формування, необхідного для забезпечення ефективної діяльності суб'єктів підприємництва, інформаційного ресурсу;
- оперативне реагування суб'єктів підприємництва на зміни та порушення умов інформаційних відносин, спроби посягань на їх інформаційні ресурси та імідж;
- своєчасне виявлення загроз інформаційному ресурсу та іміджу суб'єктів підприємництва, їх інформаційним відносинам;
- забезпечення інформаційного впливу в необхідних суб'єктам підприємництва сегментах ринку;
- підготовка персоналу суб'єктів підприємництва з питань їх інформаційної безпеки;
- оптимізація заходів та витрат пов'язаних з забезпеченням інформаційної безпеки підприємницької діяльності.

Зазначені завдання мають бути інтегровані у повсякденну діяльність суб'єктів підприємництва шляхом планової роботи як спеціальних підрозділів інформаційної безпеки, так і всіх інших, що входять до складу організаційної структури суб'єктів. Останні мають забезпечувати свою інформаційну безпеку всією сукупністю своїх економічних, інтелектуальних, технічних, кадрових можливостей.

Організація інформаційної безпеки суб'єктів підприємництва здійснюється на основі принципу централізованого управління стратегічним розвитком суб'єктів і їх безпеки, як правило, у сукупності заходів, що виконуються ними у сфері забезпечення їх безпеки.

Основними принципами тут виступають:

- *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 суб'єктами підприємництва самостійно, в межах своїх можливостей і повинні бути адекватними загрозам їх інформаційній безпеці; за результати вжитих заходів відповідальність покладається на суб'єктів підприємництва та уповноважених ними на проведення таких заходів осіб;

- *компетентність* – виконання заходів інформаційної безпеки має здійснюватися професійно, 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 суб'єктів підприємництва;

- *цілеспрямованість* – заходи інформаційної безпеки мають здійснюватися у строгій відповідності основним завданням і напрямком діяльності суб'єктів підприємництва;

- *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 суб'єктів підприємництва визначається через її відповідність встановленим вимогам, якими можуть бути:

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

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

- *конкретність інформаційної безпеки* – заходами безпеки мають бути охоплені конкретні об'єкти та дії суб'єктів підприємництва; заходи безпеки повинні бути пов'язані з конкретними операціями, угодами, відносинами, які здійснюються на даний час суб'єктами підприємництва;

- *активність інформаційної безпеки* – в арсеналі заходів інформаційної безпеки повинні бути як такі, що забезпечують захист інформаційного ресурсу та іміджу суб'єктів підприємництва, 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.

Реалізація принципів і вимог до інформаційної безпеки неможлива без конкретизації самого об'єкта безпеки. Враховуючи багатофункціональність інформації можна бачити її присутність у будь-якому матеріальному чи нематеріальному об'єкті або у будь-якому виду діяльності. Тобто, будь-який об'єкт чи діяльність можна подати інформаційно, зробити уявлення про нього на основі його інформаційних характеристик. Таким чином, беручи за об'єкт інформаційної безпеки інформацію, маємо обов'язково пов'язати її з певним об'єктом (людиною, підприємством, установою, організацією, предметом) або ж з відповідним видом діяльності. Тоді об'єктом буде виступати уже не інформація як така, а інформація про щось (об'єкт чи діяльність). Разом з тим, інформація про щось може бути об'єктом інформаційної безпеки лише тоді коли вона буде мати певну цінність (для підприємництва – комерційну цінність) і щодо неї буде проявлена зацікавленість з боку інших осіб. Враховуючи наведене, інформацію як об'єкт інформаційної безпеки можна подати наступним чином – Рис. 2.

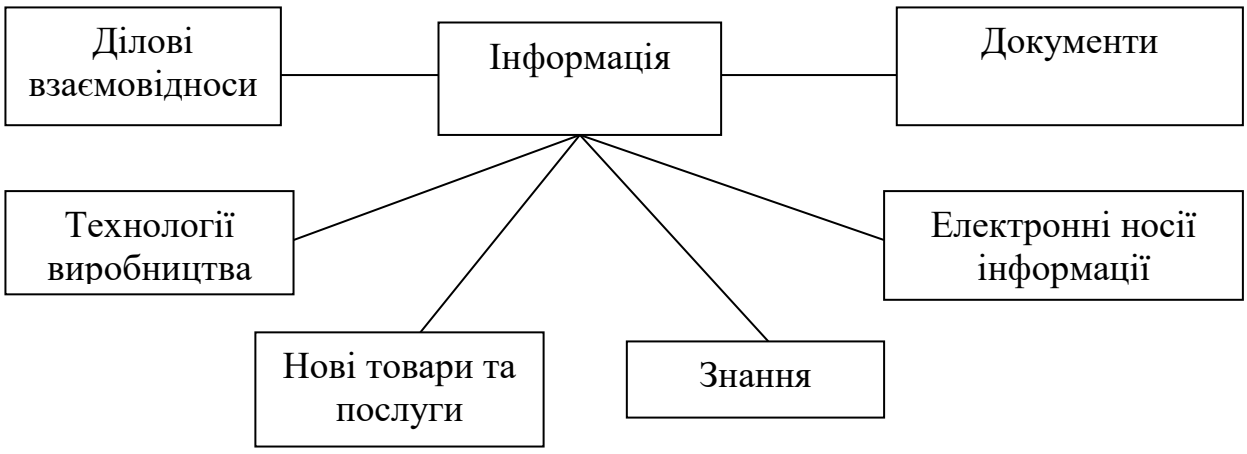

Рис. 2. Інформація як об'єкт інформаційної безпеки

У практиці забезпечення інформаційної безпеки суттєве значення має визначення її видів. Особливо це необхідно з т. з. організації інформаційної безпеки в діяльності суб'єктів підприємництва.

Аналізуючи практику інформаційних відносин суб'єктів підприємницької діяльності – підприємств та беручи до уваги роль інформації в такій діяльності, можна говорити, що інформаційна безпека підприємництва включає наступні її види:

- комп'ютерну безпеку,
- інформаційно-психологічну безпеку,
- комунікаційну безпеку т
- документаційну безпеку.

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

Інформаційно-психологічна безпека зосереджує свої зусилля у сфері знанієвої інформації та її носіїв (працівників, клієнтів, споживачів продукції суб'єктів підприємництва). Основними напрямками забезпечення інформаційної безпеки є захист знаннєвої інформації (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 суб'єктів підприємництва; 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 суб'єктів підприємництва; 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.Процес організації інформаційної безпеки підприємства: поняття, структура.

Підвалинами успіху інформаційної безпеки є грамотна її організація в діяльності суб'єктів підприємництва. На жаль необхідно констатувати, що саме організація на сьогодні є одним із найбільш слабких місць у забезпеченні інформаційної безпеки підприємницької діяльності. Немає таємниці в тому, що саме професійно організована інформаційна безпека є запорукою успіху суб'єктів підприємництва у їх інформаційних відносинах і діяльності взагалі. Організація інформаційної безпеки є елементом управління безпекою кожного із суб'єктів підприємництва. Тому цим питанням має опікуватись насамперед їх керівництво. Так, з питань організації інформаційної безпеки керівники установ суб'єктів підприємництва мають визначити мету безпеки, її основні завдання та напрямки зосередження основних зусиль; створити сприятливі умови для діяльності сил інформаційної безпеки відповідно до функцій покладених на неї; забезпечувати контроль ефективності функціонування системи інформаційної безпеки суб'єктів підприємництва. Безпосереднім організатором інформаційної безпеки є керівник підрозділу безпеки суб'єкта підприємництва, а там де він відсутній – сам керівник суб'єкта.

Аналіз практики забезпечення інформаційної безпеки в підприємницькій діяльності показує, що питанням її організації не придається 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.

За результатами узагальнення діяльності суб'єктів підприємництва по забезпеченню їх інформаційної безпеки автором запропоновано відповідну структуру процесу її організації на підприємствах, у банках та інших організаціях (Рис. 3).

Процес організації інформаційної безпеки суб'єкта підприємництва виконується на підставі глибокого вивчення умов та змісту діяльності суб'єкта, характеру його взаємовідносин на ринку та поведінки в інформаційному середовищі. Крім того, процесу організації мають передувати вивчення можливостей суб'єкта підприємництва 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 установи суб'єкта підприємництва. Точка зору керівника має бути сформована як його рішення з даного питання.

Важливим в організації інформаційної безпеки суб'єктів підприємництва залишається створення відповідної системи. Остання має розумітись як певна сукупність сил, засобів, заходів і технологій, спрямованих на забезпечення високої стійкості суб'єкта підприємництва до інформаційних загроз та ефективне інформаційне супроводження його діяльності.

Основними принципами побудови системи інформаційної безпеки мають виступати:

- *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 суб'єкта підприємництва;
- *трансформація* – система має працювати з різними видами інформації, в різних інформаційних середовищах, в будь-яких комунікаційних мережах без втрати ефективності забезпечення інформаційної безпеки суб'єкта підприємництва;
- *відновлення* – система має бути здатною в оптимально короткі терміни відновлювати свою живучість та забезпечувати виконання необхідного обсягу заходів інформаційної безпеки суб'єкта підприємництва 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 суб'єктів підприємництва. 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.

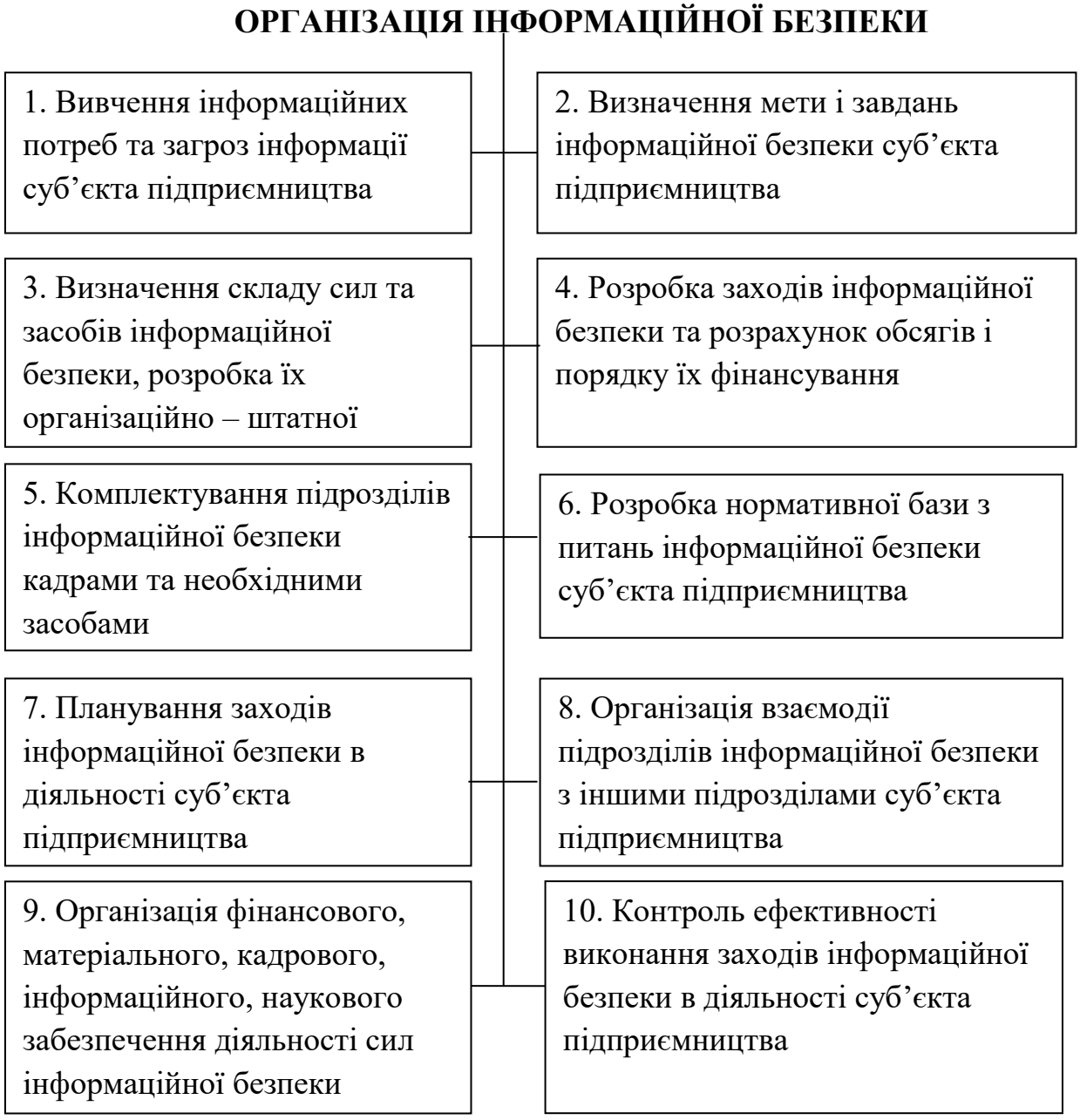

Рис. 3. Структура процесу організації інформаційної безпеки суб'єкта підприємництва

🕮 Список рекомендованої літератури

1. Конституція України : Закон України від 1996 р. *Відомості Верховної Ради України.* 1996. № 30. Ст. 141.
2. Про Національну програму інформатизації : Закон України від 1998 р. *Відомості Верховної Ради України*. 1998. № 27-28. Ст. 181.
3. Про Концепцію Національної програми інформатизації : Закон України від 1998 р. *Відомості Верховної Ради України*. 1998. № 27-28. Ст. 182.
4. Про Державну службу спеціального зв'язку та захист інформації України: Закон України від 23 лютого 2006 року. *Відомості Верховної Ради України*. 2006. № 30. ст.258.
5. Про інформацію: Закон України від 2 жовтня 1992 р. *Відомості Верховної Ради України.* 1992. № 48. Ст. 650.
6. Стратегії розвитку України : теорія і практика; за ред. О.С. Власюка. К.: НІСД, 2002, 864 с.
7. Зубок М. І. Інформаційно-аналітичне забезпечення підприємницької діяльності. К.: ГНОЗІС, 2015. 216 с.
8. Кормич Б. А. Інформаційне право. Підручник. Харків: БУРУН і К., 2011. 334 с.
9. Крегул Ю.І., Зубок М.І. Правове регулювання безпеки підприємницької діяльності: навч. посібник. К.: КНТЕУ, 2013. 216с.
10. Шпакова О. Политика информационной безопасности в Украине: правовой базис. *Актуальні проблеми міжнародних відносин*. 2008. Вип.65 (Ч. 1). С. 242-249.