МІЖРЕГІОНАЛЬНА
АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

МАУП

Методичні рекомендації
до самостійної роботи студентів з дисципліни

«ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ УПРАВЛІНСЬКОЇ ДІЯЛЬНОСТІ»

(для магістрів)

Київ – 2019

Підготовлено док.філ. у гал. екон, доцентом Середюк К.В.

Затверджено на засіданні кафедри менеджменту (протокол №7 від 19 лютого 2019 р.)

Схвалено Вченою радою Навчально-наукового інституту менеджменту, економіки та фінансів (протокол №2 від 25 лютого 2019 р.)

Середюк К.В. Методичні рекомендації щодо самостійної роботи студентів з дисципліни «Теоретико-методологічні засади інформаційного забезпечення управлінської діяльності» (для магістрів). – К. : МАУП, 2019.- 42 с.

Методичні рекомендації містять матеріали та вказівки до організації самостійної роботи студентів з дисципліни «Теоретико-методологічні засади інформаційного забезпечення управлінської діяльності», опрацювання окремих тем, питання для самоконтролю та список рекомендованої літератури.

Міжрегіональна Академія управління
персоналом (МАУП), 2019

Пояснювальна записка

Методичні вказівки до організації самостійної роботи студентів з дисципліни «Теоретико-методологічні засади інформаційного забезпечення управлінської діяльності»

В процесі підготовки магістрів важливою складовою опанування навчальною дисципліною «Теоретико-методологічні засади інформаційного забезпечення управлінської діяльності» є самостійна робота студентів за темами навчальної програми. Поруч з основними видами занять – лекціями, семінарами і практичними заняттями – вона сприяє закріпленню і поглибленню здобутих знань в процесі індивідуальної роботи з рекомендованими джерелами, формуванню навичок самостійного управління інформаційно-комунікативною сферою організації для вирішення завдань, що стоять перед нею. Будучи індивідуальним видом роботи, вона здійснюється відповідно до навчальної і робочої програм дисципліни.

Самостійна робота студента, крім засвоєння методів самостійного вивчення навчального матеріалу, становлення навичок пошуку додаткових знань відповідно до особистих здібностей кожного студента, дозволяє йому вільно орієнтуватися в інформаційному потоці за предметом вивчення дисципліни, розвивати незалежність мислення та формувати власну точку зору на питання, що вивчаються.

Самостійна робота з дисципліни «Теоретико-методологічні засади інформаційного забезпечення управлінської діяльності» починається після вступної лекції, на якій викладач дає основні рекомендації щодо методики самостійного опанування курсом.

Готуючись до самостійної роботи студент має обов’язково ознайомитися з відповідною темою курсу на основі конспекту лекцій, щоб мати загальне уявлення про досліджувану проблему, конкретне питання, підібрати рекомендовані джерела навчальної літератури. Тобто, основними формами самостійної роботи з дисципліни «Теоретико-методологічні засади інформаційного забезпечення управлінської діяльностіи» є робота з підручниками і посібниками; з науковою літературою; самостійне вивчення окремих тем і питань до семінарських і практичних занять на основі навчальної літератури і періодичних видань; підготовка реферату; підготовка до консультацій з викладачем; підготовка до заліку.

Особливо ретельно слід опрацьовувати джерела навчальної літератури. Одночасно варто працювати з декількома з них. У їх списку з кожної теми подано низку основної і рекомендованої літератури. Звичайно, зважаючи на час, він не є обмеженим та остаточним. Працюючи з джерелами, доцільно занотовувати найбільш цікаві факти, судження й висновки. При цьому обов’язково слід фіксувати посилання на автора.

При наявності незрозумілої термінології, дефініції, категорії, визначення, потрібно звертатися до відповідних словників, енциклопедій чи за консультацією до викладача.

Участь у семінарському занятті, виконання практичних завдань, написання рефератів в певний мірі є результатом самостійної роботи студента з дисципліни. Їх якість враховується при оцінюванні знань, є фактором для успішного підсумкового контролю знань під час заліку.

Тематичний план дисципліни
«Теоретико-методологічні засади інформаційного забезпечення управлінської діяльності»

Змістовий модуль (тема)	**Лекції**	**Семінарські заняття**	**Практичні заняття**	**Самостійна робота студента**
Змістовний модуль І. Загальні теоретичні та організаційні засади управління інформаційними зв'язками.				
1. Інформаційні зв'язки як складова адміністративної і соціально-виробничої систем та елемент процесу управління.	4			10
2. Інформаційні зв'язки в менеджменті та закони їх розвитку.	2			12
3. Аналіз потреб у зовнішніх і внутрішніх інформаційних зв'язках.	2	2		16
Змістовний модуль ІІ. Особливості роботи з інформацією і документами при реалізації інформаційного забезпечення управлінської діяльності.				
1. Методи та засоби збору, обробки, зберігання, пошуку і розповсюдження інформації.	4			10
2. Доступ до документів та організація їх використання.	2	2		10
3. Організація колективної роботи з документами.	2	2	2	14
4. Вимоги до комунікацій при реалізації інформаційних зв'язків.	2	2		12
5. Планування управління інформаційними зв'язками у сфері комунікацій.	2	2	2	10
6. Технології та технічні засоби передачі інформації.	2	2		8
7. Організаційно - технічні та режимні заходи безпеки інформаційних зв'язків.	2			10
8. Дотримання службової і державної таємниці в процесі реалізації інформаційних зв'язків.	2	2		10
Всього: 162 год., у т.ч.	**26**	**14**		**122**

Методичні вказівки до самостійного вивчення
дисципліни **«Теоретико-методологічні засади інформаційного забезпечення управлінської діяльності»**

<u>Змістовий модуль І.</u> Загальні теоретичні та організаційні засади управління інформаційними зв'язками.

1. **Інформаційні зв'язки як складова адміністративної і соціально-виробничої системи та елемент процесу управління.**
2. **Інформаційні зв'язки в менеджменті та закони їх розвитку.**
3. **Аналіз потреб у зовнішніх і внутрішніх інформаційних зв'язках.**

<u>Питання 1.</u> Інформаційні зв'язки як складова адміністративної і соціально-виробничої системи та елемент процесу управління.

Відомо, що процес управління організацією неможливий без внутрішнього обігу інформації між її підрозділами (структурами), без її пошуку, обміну, поширення у зовнішньому середовищі, тобто в значній мірі залежить від налагодженості інформаційних зв'язків.

Інформаційні зв'язки мають забезпечити надходження інформації до систем управління організацією та дієвість управлінського процесу в цілому. Вони можуть розглядатися як комплексно (охоплювати всі функції управління), так і по окремим функціональним управлінським діям (прогнозування й планування, облік і аналіз). Інформаційні зв'язки мають забезпечити всі види інформаційної діяльності, відповідні інформаційні процеси, в першу чергу збирання і переробку інформації, яка необхідна для прийняття управлінських рішень. Передача інформації про стан і діяльність організації на вищий рівень управління та взаємообмін нею між її підрозділами, здійснюється на базі сучасної електронно-обчислювальної техніки інформаційних технологій та інших технічних засобів зв'язку.

Сукупність інформаційних зв’язків має підготувати основу для ефективного використання інформації в управлінні. Вони повинні бути орієнтовані в першу чергу на реалізацію тих її основних властивостей, що характеризують якість і цінність інформації, тобто фінансову вартість, достовірність, повнота, точність, актуальність.

Поява телефону, радіо, телебачення, персональних комп'ютерів, локальних комп'ютерних мереж і глобальної мережі Інтернет, привели до різноманіття інформаційних зв'язків, до підвищення ролі інформації в адміністративній і соціально-виробничій сферах організації, перетворення її в ресурс успішної реалізації процесу виробництва.

Оптимальна організація інформаційних зв'язків і ефективне управління ними здатні забезпечити:

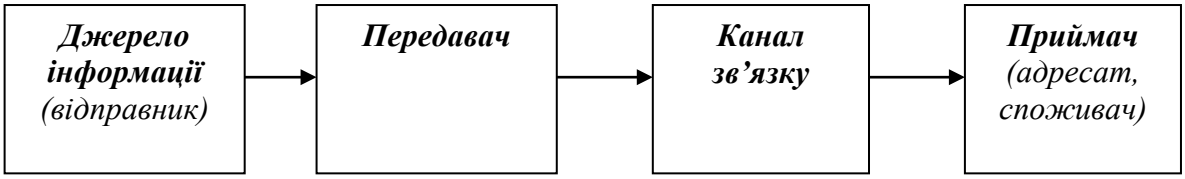
1. Економію витрат за рахунок зниження фонду заробітної плати, вартості програмного забезпечення, витрат на пошту, оформлення договорів, витрат на перерозподіл сировини.

2. Виключення можливих витрат в майбутньому - за рахунок приросту чисельності персоналу, зменшення вимог до обробки даних, знижки вартості обслуговування.

3. Можливі нематеріальні вигоди - поліпшення якості інформації, підвищення продуктивності виробництва, впровадження нових виробничих потужностей, більш дієві і достатні управлінські рішення, підвищення якості контролю, повне використання програмного забезпечення.

Поняття інформаційних зв'язків є досить широким і достатньо ємним. Воно тісно пов'язано з поняттям і терміном «інформація» і невід'ємно від них, а також процесу і схем її передачі (одержання) комунікації.

Так, навіть при простій (лінійній) схемі передачі інформації в одному напрямку (Мал. 1), в наявності певна кількість посередників, що може вплинути на тривалість її передавання, привести до спотворень.



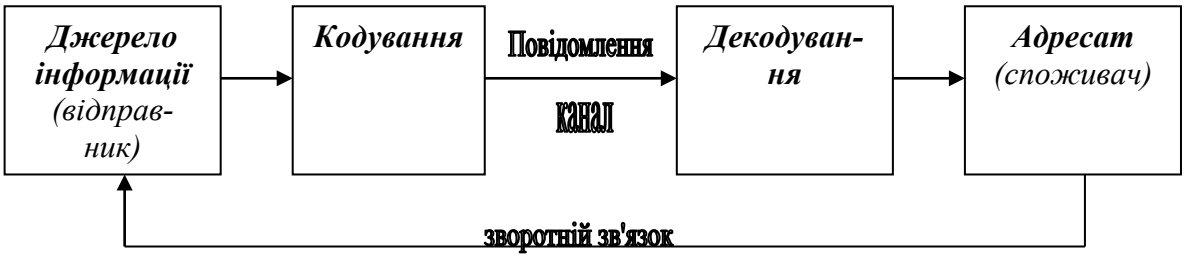
Мал.1. Процес передачі – одержання інформації.

Крім того, інформація і, відповідно, інформаційні зв'язки можуть перетворюватися в залежності від того, кому вона адресована. Так, наприклад, при її передачі керівництву (вертикальний зв'язок) відбувається не тільки її узагальнення за змістом, а при передачі підлеглому («зверху - вниз») конкретизація. Головне в цьому процесі інформаційного зв'язку - максимальна швидкість передачі при мінімальних спотвореннях. Від цього в першу чергу залежить правильність рішень, що приймаються, і як наслідок, ефективність діяльності організацій (наприклад, економічна - збільшується прибуток).

В процесі передачі - одержання інформації реалізуються комунікативні і комунікаційні зв'язки (обмін інформацією). Причому напрям цих зв'язків може бути не тільки вертикальним, а й горизонтальним, як у внутрішній, так і в зовнішній сферах діяльності організації. Звідси очевидна необхідність управління інформаційними зв'язками, оскільки вони є основою всього управлінського процесу.

Сутність інформаційних зв'язків визначає зміст і адресність інформації, яка в свою чергу визначає міру потенційних знань менеджера (керівника) про процеси і явища, їх взаємозв'язок, що відбуваються в організації. Таким чином, інформаційні зв'язки - необхідна передумова з'єднання учасників інформаційно-комунікативного процесу і наступного використання інформації для забезпечення дієвості управління. Управління інформаційними зв'язками розповсюджується на всі види інформації (економічну, технологічну, технічну тощо) та її джерела (люди, організації, документація тощо).

Базуючись на положеннях процесно-орієнтованого підходу, які припускають виділення і побудову процесів відповідно до розв'язуваних задач організації, можна виділити процеси, під які підбудовуються організаційні структури і інформаційно-технологічна підтримка. Виходячи з цього і будуються більш складні схеми передачі інформації, які існують в рамках жорстко заданих обмежень. Так, наприклад, в схемах, де на вхід процесу надходить інформаційна потреба, на виході має бути сформований інформаційний сервіс, що надається кінцевому користувачу. Такий процес протікає незалежно від організаційної структури і функціональних задач/операцій. Крім того, управління процесами передавання інформації може протікати в зворотному напрямку: від адресата (споживача) до джерела інформації (відправника). Це може бути наслідком аналізу одержаної інформації та появи нової потреби, що до цього не розглядалася чи була потрібною (Мал..2).



Мал.2. Декодування отриманої інформації.

В такій схемі слід звертати увагу на кодування інформації і вибір каналу для її передачі. Під кодуванням інформації частіше за все розуміють її , перетворення. Використовуючи різні коди, одну і ту ж інформацію можна передати усно, письмово (текст, графіка), різними мовами, за допомогою жестів, різних технічних засобів. Саме канал - це засіб передачі інформації (письмові або усні повідомлення, телефон, факс, електронна пошта тощо).

Кодування інформації, тобто її цілеспрямоване перетворення, диктується, як правило, зручністю її представлення або подальшої передачі чи визначається секретністю, обмеженістю доступу. У всіх випадках потрібно бути впевненим, що адресат зуміє її декодувати без втрат і спотворень. Для забезпечення цієї впевненості використовуються різні форми зворотного зв'язку.

Зворотній зв'язок - це сигнал, що направляється адресатом (споживачем інформації) відправнику (джерелу інформації), в якому підтверджується факт отримання повідомлення і характеризується ступінь розуміння (нерозуміння) наявної у ньому інформації. Зворотній зв'язок при організації інформаційних зв'язків за такою схемою має завчасно плануватися, бути свідомим, мати оптимальну форму, що відповідає ситуації, можливості сприйняття інформації. Стійкий зворотній зв'язок дозволяє суттєво підвищити надійність обміну інформацією, в певній мірі не допустити її втрат, викривлень, перешкод в її одержанні.

Розрізняють внутрішні і зовнішні інформаційні зв'язки. Внутрішні - це ті, що визначаються внутрішньою структурою організаціями та функціями її підрозділів. В цьому аспекті на основі процесно-орієнтованого підходу можна говорити про систему внутрішніх зв'язків, в основі яких лежать взаємозв'язки організаційних структур, функції персоналу, види документації, що є в обігу організації.

Зовнішні інформаційні зв'язки визначаються організаційними, виробничими, інформаційними тощо відносинами організації із зовнішнім середовищем. Це також певна система, що базується на зовнішній інформації. Сюди входять відомості з періодичних і спеціальних видань, дані статистичних збірок, матеріали роботи конференцій, ділових зустрічей, офіційні, господарсько-правові документи тощо.

Інформаційні зв'язки можна поділити на:

- основні і допоміжні, ті, що необхідні для забезпечення основної діяльності, виконання функцій;
- регулярні і епізодичні (формуються за необхідністю);
- первинні (базуються на інформації з першоджерел, даних первинного обліку, офіційних матеріалах) і вторинні (базуються на інформації, що була піддана певній обробці - звіти, огляди, аналітичні матеріали).

В діяльності великих господарських структур оптимізація інформаційних зв'язків є чинником нормального їх функціонування. При цьому особливої ваги набуває забезпечення їх оперативності, достовірності передачі інформації, безпеки функціонування. Створюється відповідна система внутрішньої корпоративної інформації, що вирішує завдання організації управлінсько-технологічного процесу і носить

виробничий характер. Найперше це торкається процесів забезпечення корпоративною інформацією, що циркулює внутрішніми каналами. Тут інформація по каналам інформаційних зв'язків важлива для прийняття поточних управлінських рішень. В цьому аспекті вони виступають чинником зниження витрат на виробничу діяльність і підвищення її ефективності, а їх зміст визначається потребами управлінських ланок і рішень, що вони мають приймати.

До організації інформаційних зв'язків висувають певні вимоги:

- Вона має забезпечувати потреби ефективного управління;
- Бути здатною постійно до удосконалення;
- Забезпечувати оперативність проходження інформації (найшвидше надходити до адресата) за рахунок застосував новітніх засобів зв'язку, обробки тощо;
- Бути раціональною, тобто організації інформаційних зв'язків (ефективність) - мінімум витрат на передачу інформації. Для забезпечення цієї вимоги потрібно не тільки вивчати (аналізувати) інформацію з позиції її користі для управління, а й структуру інформаційних потоків (виключення зайвих, непотрібних чи надмірних відомостей, даних);
- Передбачати обмеженість, (з метою скорочення інформаційного ланцюжка, чіткість і своєчасність реалізації (проходження) процесу передачі інформації).

Має бути налагоджена система інформаційних зв'язків – як сукупність взаємозв'язку людей, устаткування і методичних прийомів, що призначена для збору, класифікації, аналізу, оцінки і розповсюдження актуальної, своєчасної і точної інформації в сфері управління з метою вдосконалення планування, втілення в життя і контролю за виконанням управлінських заходів.

Таким чином, організація інформаційних зв'язків має постійно вдосконалюватися з урахуванням наведених вище вимог. Це є умовою підвищення її дієвості та ефективності управління. В цьому аспекті при реалізації інформаційних зв'язків важливу роль відіграють технології інформаційної діяльності, способи реєстрації, обробки, накопичення і передачі інформації, можливості її виробництва, зберігання та видачі в потрібній формі. Зазначене має входити в систему інформаційних зв'язків.

Проте, одержання інформації не є лише метою управління. Ефективна діяльність та одержання прибутку є більш високою метою. Інформаційні зв'язки виступають як кров'яна система (судини), яка забезпечує циркуляцію інформації (крові) через доставку організованої, чітко структурованої і своєчасної інформації. В організації і реалізації інформаційних зв'язків, подальше успішне управління, залежать від кваліфікації менеджера з управління інформаційними зв'язками.

В цілому на управління процесом передавання інформації, її використання впливають як індивідуальні особливості менеджера, так і специфічні організаційні вимоги, що ґрунтуються на необхідності оперувати зібраною інформацією.

Людина, яка здійснює управління інформаційними зв'язками, повинна мати знання щодо принципів відбору інформації, вміти активно її переробляти, виконувати сортування за певною оціночною шкалою, наприклад, за значущістю, за ступінню новизни та ін.. При цьому процес управління можна представити як процес послідовного прийняття рішення про можливість відбору і виділення з потоку груп документів, які відповідають певній сукупності ознак.

Тут необхідно врахувати психологічні критерії відбору інформації:

- критерій *поліментності* –орієнтує на відбір інформації, яка викликає в людському мозку найбільшу кількість думок, призводить до виникнення декількох варіантів вирішення завдання і створює велику вірогідність правильного і швидкого вибору найкращого варіанту його розв'язання;
- критерій *активності* - орієнтує на відбір інформації, яка є значущою не з наукової або технічної точки зору, а з точки зору психології мислення, тобто обумовлює народження нових думок, активно впливає на креативність мислення.

Таким чином, уміння управляти інформаційними зв'язками, розуміння природних і штучних бар'єрів на шляху інформації в організації стає сьогодні однією з найважливіших характеристик у кваліфікації менеджера.

Теми рефератів:

1. Роль інформаційних зв'язків у соціально-економічному житті суспільства.
2. Характерні риси інформаційної економіки.
3. Глобалізація інформаційних зв'язків: прояв і напрямки.
4. Інформаційний напрямок розвитку сучасного менеджменту (зміст, характеристика, приклади).
5. Структура прийняття управлінського рішення.
6. Інформаційна складова управлінської праці. Рішення як інформаційний процес.
7. Поняття інформаційної взаємодії.
8. Завдання інформаційного зв'язку.
9. Групування працівників відповідно до їх функцій в структурі інформаційних зв'язків.
10. Інформаційні форми діяльності керівника.
11. Зміст інформаційного забезпечення управління.
12. Вимоги, якім повинна відповідати інформація в процесі нформаційного зв'язку.
13. Зміст документаційного забезпечення управління. Н.Якісні критерії відбору інформації на вході інформаційної системи.
14. Психологічні критерії відбору інформації та їх вплив на результативність рішень, що приймаються.
15. Організація процесу обміну інформацією.
16. Особливості деяких видів управлінської інформації.

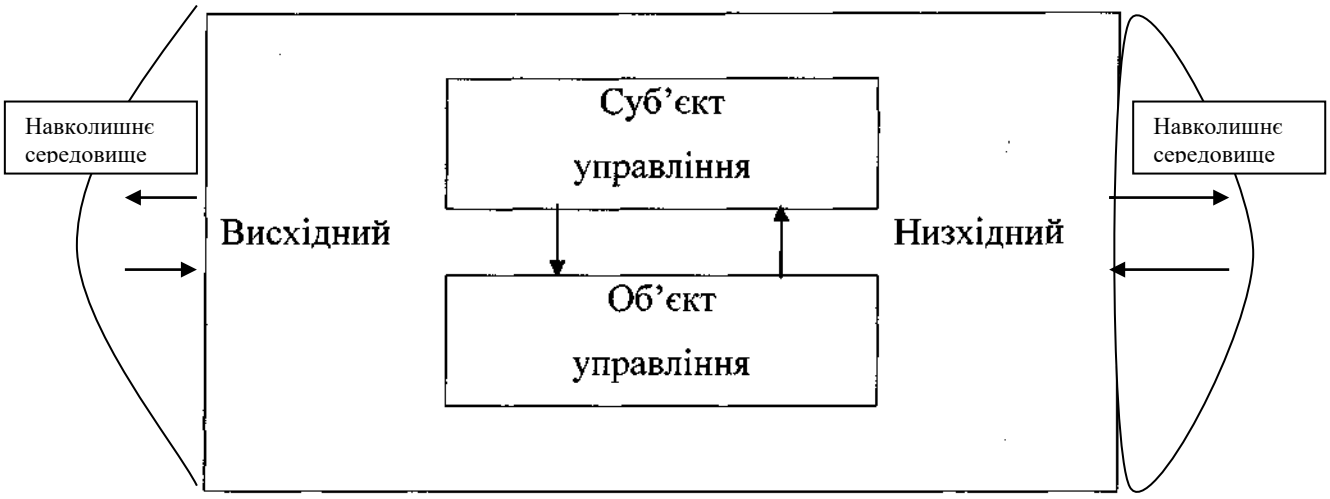
Література: ***[4, 8, 15, 17,*** *33]*.

Список використаних джерел *(Література до рефератів)*

1. http: //comin.kmu.gov.ua
2. Вплив ЗМК на демократизацію політичного життя України // Нова політика.- № 6. – 2006. – С. 26-29.
3. Колиба В.В. Національний інформаційний простір: сучасність та перспективи // Національна безпека та оборона. – 2005. – №2. – С.18.
4. Парахонський Б. Українське суспільство в добу глобалізації // Вісник НАН України.- №4.- 2006.- С.40-49.
5. Сенченко М. Основні тенденції випуску друкованої продукції у 2006 році в контексті інформаційної безпеки // Друкарство. – 2005. – С. 11.

Питання 2. **Інформаційні зв'язки в менеджменті та закони їх розвитку.**

Як відомо, сутність менеджменту полягає у розробці погоджених дій усіх об'єктів управління, встановлення узгодженості між індивідуальним роботами. Такий зв'язок суб'єктом (система, яка управляє) і об'єктом управління (підсистема, якою управляють) через інформаційні зв’язки показано на малюнку 3.



Мал..3. Інформаційні зв'язки в системі управління. .

Зв'язок здійснюється обміном інформацією. Від суб'єкта управління до об'єкта надходить потік інформації. Інформаційний потік до суб'єкта управління містить дані про стан об'єкта, про виконання одержаних команд, та реакцію на них.

На систему управління впливає також навколишнє середовище.

Таким чином, можна зробити висновок, що в основі процесу управління лежить інформація, яка передається певними каналами і таким чином забезпечуються інформаційні зв'язки. В цьому плані, характеризуючи інформацію в системі управління та інформаційні зв'язки в менеджменті, слід виділити такі головні аспекти:

- це спосіб: манера спілкування з людьми;
- це влада: мистецтво керівника. Уміння та адміністративні навички керівника;
- це ієрархія управління.

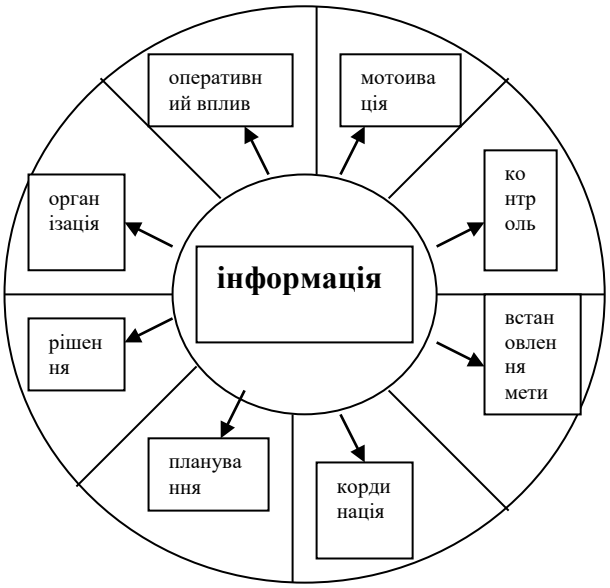
Об'єднавши всі ці окремі характеристики, можна визначити, що інформаційні зв'язки в менеджменті - це спосіб організації праці, з ефективного використовування інформаційних ресурсів, який реалізується за допомогою використання сукупності теоретичних та практичних знань, зафіксованих на носіях інформації, передаються за допомогою технічних засобів. Через інформаційні зв'язки реалізовуються певні функції в менеджменті .

Під функцією менеджменту розуміють чітко окреслене коло питань та завдань, які вирішуються певною особою чи структурним підрозділом апарату управління підприємством (організацією).

Вони поділяються на дві групи: загальні і спеціальні. Загальні функції менеджменту властиві всім рівням управління. Серед них:

- планування;
- організація;
- координація;
- мотивація;
- контроль;
- оперативний вплив;
- встановлення мети;
- рішення.

Схематично це можна зобразити так: (Мал. 4).



Мал.4. Забезпечення функцій менеджменту через інформаційні зв'язки (—► інформаційний зв'язок).

З цих позицій підприємство (організація), як система, може бути представлено сукупністю певних інформаційних зв'язків:

- інформаційні зв'язки керівників - спеціальні управлінські зв'язки, завдяки яким здійснюється керівництво, використовуючи комплекс спеціальних методів;
- інформаційні зв'язки працівників, які виконують певні функції;
- сукупність інформаційних зв'язків, що технічно забезпечують управління - організаційна та обчислювальна техніка, що використовується при управлінні;
- інформаційні зв'язки на базі документного потоку - зв'язки, необхідні для планування, організації і контролю виконання завдань, спрямованих на здійснення процесу управління організацією (підприємством).

Таким чином, інформаційні зв'язки в менеджменті - елемент управлінської діяльності, пов'язаної зі збиранням, збереженням, обробкою та передачею інформації, що потрібна для підбору та накопичення даних (відомостей), необхідних для прийняття управлінського рішення, аналізу, планування і контролю. В даному випадку менеджмент називають інформаційним і його функції реалізуються через інформаційні потреби та інформаційні запити.

Теми рефератів::

1. Типологія інформаційних зв'язків.
2. Види інформаційних зв'язків.
3. Структура інформаційних зв'язків.
4. Механізм функціонування інформаційних зв'язків.
5. Характерні риси розвитку інформаційних зв'язків в Україні.

Література: (5, 8, 22, 27, 41).

Питання 3. Аналіз потреб у зовнішніх і внутрішніх інформаційних зв'язках.

В основі раціональної системи управління, лежить низка чинників. Серед них особливе місце посідають інформаційні зв'язки суб'єктів інформаційних відносин, які мають певні інтереси і прагнуть їх реалізувати, ставлячи перед собою відповідні цілі. Їхня взаємодія й обумовлює механізми і форми організації як самих інформаційних відносин, так і відповідних інформаційних зв'язків. Так, суб'єктами інформаційних відносин згідно

Закону України «Про інформацію» є громадяни України, громадяни інших держав, юридичні особи, сама держава, міжнародні організації тощо.

З метою аналізу потреб у зовнішніх і внутрішніх інформаційних зв'язках здійснюється поділ учасників інформаційних відносин відповідно до їх ролі в процесі управління чи життєдіяльності організації, суспільства в цілому. Наприклад, за критерієм однотипності їх функцій це:

- громадяни України та інших держав;
- організації (підприємства) України та інших держав;
- органи державної (центральної) влади та відповідного галузевого управління;
- органи місцевої влади самоврядування та відповідного галузевого управління.

Наведений поділ може бути продовжено за іншими ознаками залежно від конкретних потреб чи ролі інформаційних відносин. Взаємодія зазначених суб'єктів приводить до утворення різних форм інформаційних зв'язків у політичній, економічній, духовній, науково-технічній, соціальній тощо сферах. Тобто, функціонування будь-якої організації напряму залежить від налагодженості інформаційного обміну, що реалізується через інформаційні зв'язки.

Окрім того, передача інформації про стан і діяльність організації (фірми) на вищий рівень управління і взаємний обмін нею між усіма підрозділами здійснюється в сучасних умовах на основі електронно-обчислювальної техніки та інших технічних засобів зв'язку. Для багатьох організацій така схема має виробничий характер і вирішує завдання технологічного процесу. Наприклад, для забезпечення підприємства кооперованою продукцією, що надходить від спеціалізованих підприємств. У цьому випадку інформаційні зв'язки є одним з факторів, що забезпечують процес виробництва й підвищення його ефективності і відіграють, таким чином, важливу роль у наданні відомостей для прийняття управлінських рішень.

Підвищення ступеня використання інформаційних зв'язків, відповідно й інформації, зменшення обсягу інформаційних потоків, усунення дублювання і забезпечення багаторазового використання інформації, встановлення певних інтеграційних інформаційних зв'язків має відбуватися на основі знання існуючих інформаційних потреб організації в цілому та її працівників, виявлення нових та прогнозування майбутніх.

Закономірно, що сутність інформаційних зв'язків буде визначатись змістом відповідних інформаційних потреб (потребою в інформації), яку людина чи організація має одержати, щоб ефективно виконувати свою роботу, позитивно розв'язати якусь проблему, задовольнити певний інтерес. Тобто потреба в інформації виникає через необхідність потреби в новому знанні і реалізується у сфері інформаційної діяльності через інформаційний запит, тобто замовлення одиниці інформації, що розглядається як потрібна або бажана. Саме інформаційний запит завершується використанням інформації. Використання є результатом цілеспрямованого пошуку (виконання запиту) через інформаційний зв'язок. Таким чином, створюється і реалізується послідовний ланцюжок інформаційних потреб, бажань, запитів і використання інформаційних зв'язків. Він складає так званий інформаційний цикл, якщо використання інформації відповідає потребі в ній. У випадку, коли інформація, що надійшла, не задовольняє інформаційну потребу, такий цикл має незавершений характер.

Як свідчить досвід, потреба в інформації завжди ширша за її використання. Адже далеко не всі вони (потреби) можуть бути повністю задоволені. Звідси випливає, що слід вивчати потенційні інформаційні потреби та планувати інформаційні зв'язки.

Механізмів вивчення інформаційних потреб досить і вони в основному базуються на аналізі поточних і перспективних потреб суб'єктів управління в інформації (прямі, опосередковані, документальні, спеціальні тощо), існують певні алгоритми їх визначення та реалізації (Мал..5).

Мал.5. Механізм визначення та реалізації інформаційних потреб

На систему забезпечення інформаційних потреб впливають певні чинники на мотиваційні, когнітивні, ресурсні. Між ними та інформаційними зв’язками існує прямий та зворотний зв'язок.

Мотиваційні чинники - це ступінь зацікавленості суб'єктів у задоволенні їхніх інформаційних потреб. На перший погляд, сама постановка такої проблеми може здаватися нелогічною. Але на практиці можлива ситуація, коли інтереси підприємства, фірми та окремих працівників не збігаються. Таких прикладів досить багато: від недбалого виконання своїх обов'язків чи навіть шахрайства окремих працівників до краху американської енергетичної корпорації Епгоп.

Під **когнітивними чинниками** процесу визначення та задоволення інформаційних потреб суб'єктів розуміють інтелектуальні здібності відповідних працівників, їхню здатність до нестандартного мислення, їхню кваліфікацію, професіоналізм у найширшому

розумінні цих слів.

Ресурсні чинники в системі забезпечення інформаційних потреб відрізняється від матеріально-технічних і фінансових ресурсів. Про них йдеться коли розглядаються про ресурсні чинники забезпечення процесу визначення потреб суб'єктів у інформації та можливості їх задоволення. Адже за умов однакової кваліфікації та мотивації працівників кращі можливості задоволення власних інформаційних потреб матимуть суб'єкти з вищим рівнем матеріально-технічного та фінансового забезпечення. В аспекті інформаційних зв’язків до них додаються ті, що пов’язані кваліфікацію працівників як специфічного виду ресурсів.

Аналіз розвитку потреб в інформаційних зв'язках доцільно проводити через систему оцінки інформаційних потреб – так званий факторний аналіз. Тут слід враховувати головні ознаки інформаційних потреб:

1. **Тематика проблеми, яку треба розв'язати.** Вона задається набором **ключових понять (слів),** на підставі яких здійснюється пошук інформації і визначаються інформаційні зв'язки.
2. **Визначення глибини аналізу (виокремлення) обраної теми** за різними ознаками - хронологічні, предметні, географічні тощо.
3. **Функції використання одержаної інформації:**

- функція пошуку даних - передбачає отримання суб'єктом заздалегідь наміченої інформації довідкового характеру;
- функція оперативної поінформованості - передбачає отримання суб'єктом регулярних повідомлень про сучасну ситуацію;
- дослідницька функція - передбачає отримання інформації для проведення глибокого дослідження у новій для суб'єкта сфері знань, діяльності тощо;
- ознайомча функція - передбачає одержання суб'єктом базової інформації, необхідної для розуміння проблеми суб'єктом;
- стимулююча функція - передбачає отримання суб'єктом інформації, необхідної для генерації нових ідей, отримання нових стимулів для подальшої інтелектуальної діяльності.

4. **Характер подальшого використання отриманої інформації** -наприклад, теоретична, довідкова, статистична, методологічна тощо. Ця характеристика за формальними ознаками близька до функції використання інформації, але має більш інваріантний (незмінний) характер, стосується перш за все властивостей власне інформації.
5. **Хронологічне охоплення подій,** тобто період часу, за який збирається інформація для її подальшого використання. Ця ознака пов'язана з обсягом необхідної інформації і залежить у першу чергу від специфіки завдань, які треба вирішити.

Перелічені ознаки (характеристики) інформаційних потреб, не обтяжені суб'єктивним впливом відправника інформації. І тому саме вони відіграють основну роль для характеристики як кожної конкретної інформаційної потреби, так і відповідних інформаційних зв'язків.

Теми рефератів:

1. Обумовленість потреб організації в інформаційних зв'язках.
2. Види потреб організації в інформаційних зв'язках.
3. Методи вивчення потреб організації в інформаційних зв'язках.
4. Зв'язок інформаційних потреб користувачів інформації та інформаційних зв'язків для їх задоволення.
5. Аналіз потреб організації у зовнішніх і внутрішніх інформаційних зв'язках.

Література: [11, 25, 35, 37, 42].

<u>Змістовий модуль ІІ.</u> Особливості роботи з інформацією і документами при реалізації інформаційного забезпечення управлінської діяльності

1. Методи та засоби збору, обробки, зберігання, пошуку і розповсюдження інформації.

2. Доступ до документів та організація їх використання.

3. Організація колективної роботи з документами.

4. Вимоги до комунікацій при реалізації інформаційних зв'язків.

5. Планування управління інформаційними зв'язками у сфері комунікацій.

6. Технології та технічні засоби реалізації інформаційних зв'язків.

7. Організаційно - технічні та режимні заходи безпеки інформаційних. зв'язків.

8. Дотримання службової і державної таємниці в процесі реалізації інформаційних зв'язків.

<u>Питання 1.</u> Методи і засоби збирання, обробки, зберігання, пошуку і поширення інформації.

В розвитку підприємства (фірми, бізнесу) значну роль відіграє його інформаційна інфраструктура. В конкурентній боротьбі вирішального значення набувають питання, що пов'язані зі збором, обробкою, зберіганням, пошуком і поширенням інформації, тобто налагодженістю процесів, через які відбувається активна робота з інформацією. Через них підприємець відбирає з множини потоків ту інформацію, яка відповідає цілям його діяльності, сприяє відпрацюванню чи реалізації ідей та завдань. Його знання через інформаційні зв'язки перетворюються в повідомлення, які організують виробничі, торговельні чи інші процеси.

<u>Теми рефератів :</u>

1. Збирання інформації як інформаційний процес та структура його інформаційних зв'язків.
2. Обробка інформації як інформаційний процес та зміст його інформаційних зв'язків.
3. Пошук інформації як інформаційний процес та особливості його інформаційних зв'язків.
4. Поширення інформації як інформаційний процес.

Література: (6, 13, 37, 44).

***<u>Питання 2.</u>* Доступ до документів та організація їх використання**

У діяльності будь-якої організації важливе місце займає робота з документами, які необхідно одержувати ззовні, готувати всередині організації, реєструвати, передавати працівникам, контролювати виконання, вести довідкову роботу, зберігати й надсилати у зовнішнє середовище. Саме тому організація роботи з документами є важливою складовою частиною процесів управління і прийняття управлінських рішень, яка істотно впливає на оперативність, економічність і надійність функціонування апарату управління, культуру праці управлінського персоналу та якість управління. У зв'язку з цим інформаційні зв'язки та інформаційні потоки повинні являти собою чітко керований і легко відстежуваний процес, в основі якого має лежати типовий інформаційний об'єкт, що фіксує і регламентує діяльність. Таким типовим інформаційним об'єктом є документ, а більш ширше – документальне джерело. *<u>Документ</u>*, в загальному розумінні, трактується як засіб закріплення різними способами на спеціальному носієві інформації про факти, події, явища реального світу чи мислиневої діяльності людини. Інформацію, у вигляді конкретних фактів, фактичних подій чи їх сукупності, зафіксовану в певній знаковій формі на будь-якому матеріальному носієві, також містять *<u>фактографічні документи</u>* (фактографічні джерела). Любе фактографічне повідомлення завжди представлено у

вигляді документа, але співвідносяться вони як частина і ціле.

Документи, що є в обігу у сфери соціальної комунікації, можуть бути різних типів і видів. Так, наприклад, за ознакою знакової форми представлення розрізняють документи:

- текстові (знак – алфавіт природної форми) – твори друку;
- іконічні (знак відбиває об'єкт, що позначає) – малюнки, фотографії, картини, діапозитиви, кінострічки тощо;
- ідеографічні (знак – умовна позначка) – географічні карти, атласи, ноти, схеми, креслення тощо;
- трьох вимірів (знак – сам матеріальний об'єкт) – музейні експонати, історичні реліквії, зразки мінералів, порід тощо;
- машинозчитувані (знак – спеціально розроблений код) – магнітні стрічки, магнітні диски тощо.
- аудіальні (фонетичні, ті що звучать) – різні види звукозапису.

Для будь-якої організації життєво важливо постійно вдосконалювати *документаційне забезпечення управління (ДЗУ)*. На жаль, іноді воно часто здійснюється стихійно, без урахування існуючої нормативної бази і досвіду вдосконалення документаційного забезпечення управління.

Із збільшенням масштабів підприємства і кількості його співробітників питання про ефективність ДЗУ стає все більш актуальним. Основні проблеми, які при цьому виникають:

- керівництво не володіє цілісною картиною того, що відбувається на підприємстві;
- структурні підрозділи, не маючи інформації про діяльність один одного, не можуть ефективно працювати через незлагодженість, знижується якість обслуговування клієнтів і здатність організації підтримувати зовнішні контакти;
- як наслідок, спостерігається падіння продуктивності праці і виникає нестача ресурсів: людських, технічних, комунікаційних та ін.;
- доводиться розширювати штат, вкладати кошти в обладнання нових робочих місць, приміщень, комунікацій, навчання нових співробітників;
- для виробничих підприємств збільшення штату може спричинити зміну технології виробництва, що в свою чергу, буде вимагати додаткових інвестицій.

Вирішенню цих проблем в значній мірі сприяє *автоматизація діловодства*. Система автоматизації діловодства включає засоби і правила створення документів, ведення електронного архіву, підтримки документообігу і спирається на програмно-технічні платформи підприємства. Всі інші складові управління повинні ґрунтуватись на системі ведення діловодства з метою ефективного використання інформації для досягнення поставлених завдань і вирішення проблем, які стоять перед організацією. З точки зору комплексної автоматизації діяльності підприємства прикладні інформаційні системи повинні саме спиратись на програмно-технічні платформи і систему автоматизації діловодства. Таким чином, перед підприємством, яке прагне створити ефективне середовище обробки інформації, постають два важливих завдання:

- вдосконалення всієї роботи з підготовки та обробки документальної інформації шляхом створення механізму ДЗУ;
- вибір правильної стратегії автоматизації;

Таким чином, доступу до документів, ефективній організації їх використання, сприяє якісна організація документообігу, відповідне документаційне забезпечення управління різними видами інформації, раціональні інформаційні зв'язки.

Теми рефератів:

1. Інформаційне обслуговування, характеристика та види.
2. Документація та діловодство в організації як основа реалізації інформаційних зв'язків.

3. Документаційне забезпечення управління, характеристика та види.
4. Організаційно-розпорядча документація організації, характеристика та види.

Література: (3, 11, 38 , 41)

<u>Питання 3.</u> **Організація колективної роботи з документами.**

Колективна робота з документами в організації являє собою сукупність процесів, які забезпечують ефективний доступ до інформації і інформаційно-комунікаційні процеси, використання і розвиток наявних інформаційних ресурсів. Зміст колективної роботи з документами в організації в значній мірі визначається взаємодією з оточуючим зовнішнім середовищем і внутрішньою взаємодією між її елементами через інформаційні зв'язки. *В сучасних умовах ця взаємодія ґрунтується на різних моделях «електронних офісів»*, сформульованих ще наприкінці 80-х років:

- *Інформаційна модель* – орієнтована на інформацію як ресурс, який виробляється і використовується у процесі функціонування системи управління, спрямована на розв'язання інформаційних проблем, раціоналізацію та інтеграцію інформаційних процесів, поліпшення організаційної структури, підвищення ефективності роботи у цілому;
- *Комунікаційна модель* – спрямована на інформатизацію управління у вигляді комплексної системи, яка охоплюєорганізацію апарату управління разом з персоналом, організаційні зв'язки, методи роботи, тобто є моделлю організаційної системи управління як складової системи соціальних комунікацій;
- *Соціотехнічна модель* – спрямована на проектування автоматизованих систем з певними параметрами інформаційних потоків, та типами комунікацій. В ній мають враховуватись також соціально-психологічні особливості організації, у якій буде функціонувати проектована система. У контексті соціотехнічного підходу кінцеві результати роботи організації залежать не в останню чергу від взаємовідносин людей, їх ціннісних орієнтацій.

Проте, навіть в "електронному офісі", де працівника оточують різноманітні засоби інформатизації із новими можливостями, які забезпечують одержання і видачу основних видів повідомлень і даних, важливим є налагодженість традиційних інформаційних потоків.

Розрізняють чотири *<u>види інформаційних потоків</u> у* організації:

1. Обмін між організацією та зовнішнім середовищем (маркетинг, реклама, зв'язки з громадськістю).

2. Міжрівневий обмін інформацією в організації:

- низхідні потоки інформації, якими повідомляють підлеглим про поточні завдання, конкретні доручення, зміну пріоритетів та ін.;
- висхідні потоки інформації - звіти про виконання завдань, пропозиції з удосконалення технології та ін., за допомогою яких керівництво інформують про поточні та можливі проблеми, про можливі варіанти рішень.

3. Горизонтальний обмін інформацією:

- наради керівників суміжних підрозділів, задіяних у виконанні спільних завдань;
- наради керівників підрозділів, які мають схожі виробничі завдання;
- робота у межах робочих груп (управління проектом).

4. Неформальний обмін інформацією:

- обговорення виробничих питань під час неформальних зустрічей (під час обідньої перерви, святкових заходів та ін.);
- чутки, основною, причиною яких є дефіцит офіційної інформації.

Дослідження свідчать, що чутки бувають на 80-90% точними (за винятком, випадків надто емоційно забарвленої інформації). Чутки є надзвичайно впливовим чинником.

Аналіз схем інформаційних потоків на рівні елементів інформації (на змістовому рівні) дозволяє відстежити шляхи документів (інформаційних зв'язків), тобто виявити

моменти їх створення, порядок об'єднання, *розлучення* в процесі проходження, і таким чином, обсяги, характер, терміни зберігання, затримки в обробці, передачі, викликані поганим розподілом функцій чи обов'язків. Результати аналізу використовують для побудови іншої, більш раціональної і логічної схеми документообігу.

Теми рефератів:

1. Інформаційно-технологічний простір організації.
2. Інформаційні потоки в організації, характеристика та види.
3. Бар'єри на шляху інформаційних потоків в організації.
4. Заходи з удосконалення інформаційних зв'язків в організації.

Література: ***(3, 4, 11, 32, 44)***

Питання 4. **Вимоги до комунікації при реалізації інформаційних зв'язків.**

Кожне підприємство, яке функціонує як відкрита система, потребує ефективних інформаційних зв'язків, щоб отримувати адекватну інформацію та мати змогу приймати відповідні управлінські рішення. В цьому процесі інтегруючим фактором є комунікація. Відповідно до цілей управління вона спрямовує інформаційні потоки від однієї ланки до іншої. Оскільки під інформаційним потоком розуміють цілеспрямований рух інформації через інформаційні зв'язки, то до комунікацій висувають певні вимоги при їх реалізації. В загальному плані вона має бути раціональною (виключає дублювання), оптимальною (короткі шляхи проходження), ефективною (забезпечувати всі потреби рівнів внутрішньому і зовнішньому середовищі).

Поняття комунікації. Комунікація має кілька значень:

- це шляхи сполучення (наприклад, повітряні або водні комунікації);
- це форма зв'язку (радіо, телеграф);
- це процес передачі інформації за допомогою технічних засобів – засобів масової інформації (радіо, телебачення, преса, кінематограф);
- комунікація виступає як акт спілкування, зв'язок між двома або більше індивідами, повідомлення інформації однією особою іншій.

Отже, комунікація - це не спілкування в усьому комплексі і багатогранності, а лише акт спілкування. Очевидно, що цей «акт» також має соціальну природу і соціальний статус. Визначення терміну «комунікація» починається від характеристики численних інформаційних систем передачі людської мови, сигналів і зображень. Згідно з цим термін «комунікація» означає «міру участі» в процесі споживання, обміну та використання інформації. Але разом з тим знаходитися у стані комунікації – це не просто передавати й одержувати інформацію. В процесі комунікації утворюється комунікативне співтовариство. Воно характеризується відносинами єдності, взаємозв'язку, взаєморозуміння.

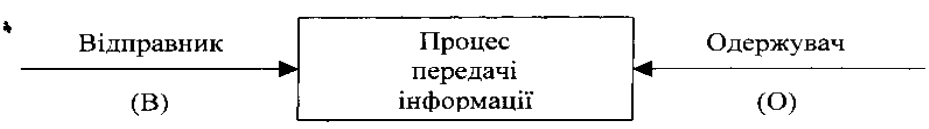
Є й інші грані комунікації. Це:

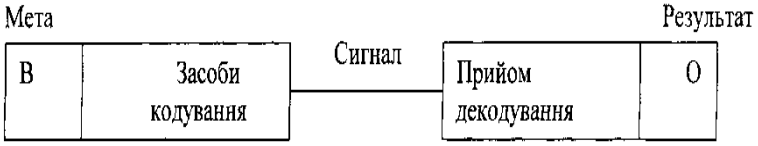
- координація з приводу-прийому та передачі інформації;
- узгодженість цінностей: оцінок і процесів розуміння;
- організація процесу зв'язку між індивідами.

Таким чином, комунікація як акт спілкування має свої особливості.

В більш вузькому, соціально-психологічному розумінні, комунікація - це процес передачі інформації від відправника до одержувача. Комунікація має певні складові частини. Найпростіше уявлення про структуру комунікації дає така схема:

Наступна характеристика процесу комунікації - цільова. Характер спілкування (передача інформації, обмін діяльністю, вміннями, навичками) визначає особливості акту спілкування - комунікації. Тоді схема комунікації матиме такий вигляд (мал.6):





Мал.6 Структура комунікації.

В структурі комунікації потрібно розрізняти мету від спонукаючого мотиву. Мета - це ясний і чіткий (часто раціонально обґрунтований) намір. Спонукаючий мотив - прихований намір. У прихованому мотиві слід розрізняти особисті цілі відправника та одержувача, наміри видати бажане за дійсне.

Таким чином, комунікація - це процес двостороннього обміну ідеями та інформацією, який веде до взаємного розуміння. Термін «комунікація» походить від латинського слова («communication»), яке означає «спільне» або «розділене між усіма». Якщо не досягається взаєморозуміння, то комунікація не відбулася.

Проте сам факт обміну інформацією ще не свідчить про комунікацію, оскільки інформація, що передається, може бути незрозуміла для того, хто її отримує.

В теорії управління під комунікацією розуміють процес обміну інформацією між двома або більше особами, який забезпечує їх взаєморозуміння. Основна роль комунікацій полягає у поєднанні всіх функцій менеджменту, в досягненні бажаної поведінки окремих осіб чи колективу в організації.

Управління комунікаційними процесами в організації включає:

- пошук та визначення перешкод на шляху до ефективної комунікації;
- розробку і реалізацію способів усунення таких перешкод і підвищення ефективності комунікаційних процесів.

Існує багато факторів, що перешкоджають здійсненню ефективної комунікації, основними з яких є:

1. Фільтрація. Коли робітник говорить те, що бажає почути його керівник - він фільтрує інформацію. Фільтрація є функцією: а) конфлікту між сферами компетенції; б) конфлікту інтересів і потреб відправника і одержувача повідомлення; в) висоти структури організації (чим вище рівень управління, тим більше умов для фільтрації); г) отриманого досвіду попередніх негативних комунікацій.

2. Вибіркове сприйняття. Одержувач краще сприймає ту інформацію, яка відповідає його потребам, мотивації, досвіду та іншим особистим характеристикам. Ступінь зацікавленості в отримуваній інформації визначається його очікуваннями, а, отже, і визначає характер декодування інформації.

3. Семантичні бар'єри. Однакові слова мають різне значення для різних людей. Вік, освіта, культурне середовище - три найбільш важливих фактора, які впливають на значення слів, що використовуються в процесі комунікацій. До організації люди приходять з різних типів середовища. Горизонтальні комунікації між спеціалістами одного профілю сприяють виникненню їх власного жаргону або специфічної технічної мови, яка незрозуміла іншим. У великих організаціях, які мають філіали в різних країнах, використовуються терміни, специфічні для відповідного регіону. Все це врешті-решт призводить до виникнення семантичних бар'єрів.

4. Поганий зворотній зв'язок.

5. Культурні відмінності (розбіжності) між відправником і одержувачем інформації.

6. Інформаційні перевантаження. Вони виникають внаслідок неможливості ефективно реагувати на всю інформацію, що отримується. Виникає потреба відсіювати найменш важливу інформацію та залишати тільки найсуттєвішу.

Створення ефективних комунікацій як усередині, так і поза організацією досягається за допомогою добре організованого комунікативного процесу.

Теми рефератів:

1. Види інформаційних повідомлень.
2. Комунікаційні потреби організації.
3. Основні підходи до класифікації комунікацій.
4. Типи комунікацій.
5. Види комунікацій.
6. Визначення та характеристика інформаційних комунікацій.
7. Визначення комунікаційного процесу.
8. Інформаційні зв'язки в комунікаційному процесі.
9. Сучасні комунікаційні стратегії.

Література: (3, 4, 11, 32, 44)

Питання 5. **Планування управління інформаційними зв'язками у сфері комунікацій.**

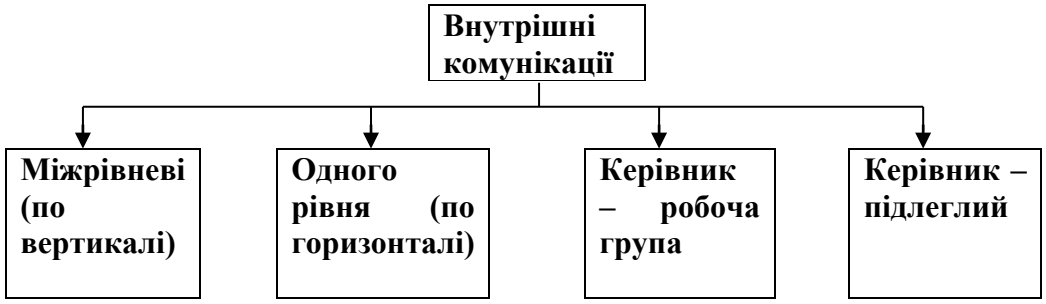
Для забезпечення ефективності системи управління, мінімізації витрат часу і заощадження інформаційних ресурсів організації, необхідно планувати інформаційні зв'язки. Необхідність планування обумовлюється як загальноекономічним (з погляду загальної теорії і природи економічних відносин), так і конкретно-управлінським (як одна із функцій менеджменту) характером діяльності підприємства, їх тісною взаємопов'язаністю, що базується на загальних умовах господарювання. Планування у сфері комунікацій надає можливість підготовки до майбутніх дій, умов; прояснює проблеми, що виникають; поліпшує координацію функції в організації; збільшує можливості забезпечення підприємства необхідними інформаційними ресурсами; сприяє більш раціональному використанню інформації.

Для прийняття рішень про зміст і характер планування, стратегії здійснення обміну інформацією із зовнішнім середовищем і забезпечення внутрішніх функцій управління через обмін інформацією, слід проаналізувати комунікаційні потреби організації.

Комунікаційні потреби організації залежать від:

- характеристик зовнішнього середовища організації (динамічність, складність, невизначеність);
- задач, розв'язуваних організацією (наприклад, якщо ставиться задача випустити якісно новий товар або послугу, захопити нові ринки збуту, здійснити модернізацію виробництва, диверсифікувати діяльність, то потреба в комунікаціях різко зростає);
- основних характеристик організації - масштабів, структури, сфери діяльності, характеру виробляємої продукції (послуг), рівня диверсифікованості, позиції в галузі і т.д.

Найбільш значний обсяг комунікацій, особливо в складних організаціях, складають внутрішні комунікації (мал.7).



Мал.7. Внутрішні комунікації організації

Комунікаційна мережа організації включає горизонтальні, вертикальні і діагональні зв'язки. Вертикальні зв'язки встановлюються між керівником і виконавцями. Прикладом

таких зв'язків є ланцюг команд (зверху вниз) і надання звітної інформації (знизу нагору). Горизонтальні комунікації існують між підрозділами організації або її членами, що належать до одного рівня організаційної структури. Діагональні комунікації - це зв'язки з підрозділами інших рівнів організації, що не відносяться до вертикальних зв'язків. Групи з рівною чисельністю можуть мати різні типи комунікаційних мереж. При формальному, централізованому типі всі комунікації здійснюються через керівника групи. Тут забезпечуються висока швидкість і точність передачі, гарна організованість і чітко виражене лідерство. Однак при цьому керівник "придушує" ініціативу виконавців. При максимально децентралізованому типі всі члени групи мають рівне число комунікаційних зв'язків. Це дозволяє досягти гарного мікроклімату в колективі. Але комунікації при такому типі мережі характеризуються повільною швидкістю, низькою точністю, слабкою організованістю, відсутністю лідерства.

Централізований тип комунікацій більш ефективний при вирішенні порівняно простих, добре структурованих задач. При вирішенні складних задач, що вимагають урахування думок усіх членів групи, більш ефективним виявляється звертання до децентралізованих, чи відкритих, комунікацій.

Основні проблеми в організаційних комунікаціях пов'язані з неефективною структурою організації. Тут можливі два полюси. Перший полюс представлений ситуацією, коли організаційна структура надмірно розтягнута. При цьому необґрунтовано зростає число рівнів управління, формується дуже довгий ланцюг команд. Декомпозиція основних цілей організації, їхня конкретизація для окремих рівнів управління і підрозділів організації ускладнює комунікації. Можливо ненавмисне перекручування звітної інформації внаслідок її руху по вертикалі. Наявність конфліктів робить дуже ймовірним навмисне перекручування інформації.

Другий полюс може бути представлений ситуацією, коли організаційна структура є необґрунтовано плоскою. Порушення норми керованості може привести до інформаційних перевантажень, особливо на вищому рівні управління. Не існує єдиних правил, які можуть бути застосовані для всіх організацій для встановлення ефективних комунікацій. Для цілей оцінки комунікації в організації найкраще розглянути ті перешкоди, що звичайно асоціюються з посилкою і прийомом переданих блоків інформації в організації. Розуміння всіх цих спотворюючих факторів є основою поліпшення комунікаційної системи. Зневага й ігнорування цих факторів може привести до уповільнення, громіздкості і перекручування, а то і до повної помилковості переданих блоків інформації.

Отже, комунікація - це процес обміну інформацією, що включає суб'єкти комунікації (відправника й одержувача), спосіб комунікації й об'єкт комунікації (передану інформацію). Ефективна система комунікацій дозволяє мінімізувати часові витрати і заощадити організаційні ресурси компанії.

При розробці плану комунікацій, беруть до уваги такі чинники:

1. Цілі комунікацій.
2. Комунікаційне середовище.
3. Управлінська ситуація.
4. Відправник повідомлення.

Цілі комунікацій. Найважливіший перший крок, коли визначаються цілі комунікацій, які необхідні для:

- інформування чи збору інформації;
- впливу на ставлення до організації;
- впливу на поведінку комунікаторів.

Інформування лише в окремих випадках є єдиною метою. Передбачається, що певним чином воно повинно впливати на зміну поведінки адресата. Наукові дослідження показали, що зміна ставлення часто є необхідною умовою зміни поведінки, тому здійснення впливу та ставлення аудиторії часто є метою комунікації.

Комунікаційне середовище. Аналіз включає дослідження його структури та

визначення профілів середовища. Аналіз аудиторії вимагає визначення:

- первинної аудиторії (людей, які приймають рішення або діють, спираючись на факти, що містять у повідомленні);
- вторинної аудиторії (людей, на яких впливають ці рішення чи дії);
- безпосередньої аудиторії (людей, які безпосередньо скеровують передачу повідомлення).

При виробленні плану аудиторія відповідно структурується. Крім загальних стандартних характеристик (вік, стать, освіта) входять ще й такі:

1. Фактична (в тому числі і неформальна) організаційна роль аудиторії (у випадках, коли те, що вона робить, є важливішим від її статусу).
2. Відомості про те, яким комунікаційним засобам надається перевага (наприклад, одні люди віддають перевагу коротким доповідям, інші - великим і т.п.).
3. Аудиторія обізнана з цією проблемою.
4. Зацікавленість аудиторії цією проблемою (іноді зацікавленість швидко згасає і для її підкріплення повідомлення повинно містити інформацію, яка привертає увагу аудиторії).
5. Чого аудиторія потребує від цього повідомлення (широкої інформації, пояснень, критичного розгляду інших варіантів тощо).
6. Який вплив повідомлення матиме на аудиторію.

Аналіз управлінської ситуації. Наведемо ряд чинників, які беруться до уваги:

1. Стиль лідерства (в установі, де діє автократичний стиль керівництва і централізовано приймаються рішення, директор є первинною аудиторією незалежно від того, кому адресоване повідомлення і який його зміст, стиль, тон тощо).
2. Політична атмосфера (у високополітизованій ситуації важливим є нюанси у словах і тоні).
3. Організаційний клімат.
4. Організаційний стан (упродовж критичної ситуації здатність організації отримувати й інтерпретувати повідомлення швидко зменшується, тому потрібно мати підготовлений план, який передбачає процедуру комунікацій в умовах критичної ситуації).
5. Організаційна культура (ступень офіційності, формалізації організації передбачає відповідний стиль спілкування, який відрізняється, скажімо, в міністерстві оборони та в міністерстві культури).

Відправник повідомлення. Останній ситуаційний чинник передбачає ідентифікацію особи (організації), від імені якої надсилається повідомлення. Вона повинна проаналізувати свої характеристики для визначення певного підсвідомо сприйнятого засобу комунікацій, домагаючись власних переваг. Численні дослідження показали, що той, кого аудиторія сприймає з найбільшим ступенем довіри, здатен продукувати значно більший ефект щодо зміни громадської думки, аніж той, кого аудиторія сприймає з меншим ступенем довіри.

Вибір засобу передачі повідомлення. Немає правильного чи неправильного шляху для надсилання повідомлення, оскільки він залежить від мети спілкування, аудиторії, того, хто надсилає повідомлення, і від ситуації. Проте наукові дослідження дозволяють акцентувати увагу на таких чинниках аудиторії та змісту:

- усне спілкування, що передбачає зворотній зв'язок і є засобом, якому надається перевага на нижніх щаблях спілкування в організаціях;
- молоді люди, які звикли до перегляду відео програм, віддають перевагу коротким "здоровим" повідомленням;

письмова, фінансова, технічна інформація сприймається ефективніше;

- письмові комунікації більш ризиковані, коли залучаються політичні, правові, адміністративні та інші чинники;
- письмові повідомлення виглядають більш офіційно, тому важче змінити їх зміст

чи відректись від них тощо.

Створення повідомлення. Ключовими елементами, які беруться до уваги при створенні повідомлення, є форма подачі, зміст, стиль, побудова, тон та рівень деталізації:

- деякі слова викликають певну реакцію аудиторії і можуть провокувати непередбачену реакцію;
- зміст повідомлення зумовлюється метою спілкування і знаннями про аудиторію та її потреби;
- якщо зміст повідомлення важкий для сприйняття, то стиль викладу повинен бути якомога простіший;
- залежно від аудиторії вибирати індуктивний чи дедуктивний метод;
- фактор часу.

Для досягнення мети комунікації передусім необхідно завоювати увагу аудиторії. Якщо увага здобута, то можна зосередитись на з'ясуванні рівня розуміння і мотивації аудиторії до сприйняття аргументів:

- завоювання уваги залежить від багатьох чинників: голос, зовнішній вигляд, стиль, початок дискусії, новизна доповіді;
- розуміння аудиторією суті повідомлення залежить від структури, яскравості, експресивності повідомлення.

Теми рефератів:

1. Основні методи поширення інформації про діяльність організації.
2. Етапи розробки плану комунікацій в організації.
3. Вибір засобу передачі повідомлення.

Література (4, 19, 27, 32, 42)

***Питання 6*. Технології та технічні засоби реалізації інформаційних зв'язків.**

Організації, як правило користуються різними засобами для комунікацій із складниками свого зовнішнього оточення. З існуючим та потенційними споживачами вони, наприклад, спілкуються з допомогою реклами та інших програм просування товарів на ринок. У сфері відносин із суспільством першочергова увага надається створенню певного образу, "іміджу" організації на місцевому, загальнонаціональному або міжнародному рівні. Отже всередині організації відбуваються обговорення, збори, телефонні переговори, циркулюють службові записки, інша документація. Такі процеси забезпечують засоби управлінського зв'язку. До них відносяться: телефонний зв'язок, стільникові телефони, модеми. В сучасних умовах найбільш розповсюджуються системи мобільного зв'язку. При їх виборі слід враховувати:

- Територіальний фактор.

Усі мобільні радіосистеми мають обмеження щодо розташування абонементського приймально-передавального пристрою відносно базових станцій, що обумовлено швидким затуханням електромагнітних хвиль УКВ-діапазону при наявності перепон на місцевості. Тому при виборі системи зв'язку необхідно ознайомитись із картою впевненого прийому сигналу і порівняти її з маршрутами передбачуваних переміщень. Для абонентів, які бажають використовувати свій абонентський пристрій в далеких поїздках, важливим є забезпечення деяких систем можливістю переключення на базові станції інших операторів (роумінг).

- Коло потенційних співрозмовників.

Якщо велика частина переговорів відбувається в рамках вузького кола абонентів, то краще обладнати їх системою зв'язку з обмеженими можливостями виходу на зовнішні телефонні лінії.

- Необхідність конфіденційності зв'язку.

Не існує мобільних систем, які забезпечують абсолютну конфіденційність, можна говорити лише про її ступінь.

- Потребу в додаткових видах обслуговування.

Можливість оперативної передачі інформації і прийому фактів, одержання даних із корпоративної або глобальної мережі підтримується не всіма операторами мобільного зв'язку. Крім засобів передачі даних деякі провайдери надають своїм абонентам головну поштову скриньку, можливість переадресування дзвінків, конференц-зв'язок.

- Радіоподовжувачі.

Радіоподовжувачі дозволяють використовувати домашню або офісну стаціонарну телефонну лінію в мобільному варіанті. З радіотелефоном можна віддалятися на декілька сотень метрів. Радіоподовжувач передбачає наявність стаціонарного телефону, що дозволяє використовувати один тюнер в офісі і на виїзді.

- Транкінговий зв'язок.

Корпоративний зв'язок, призначений для роботи, переважно, в рамках однієї групи, тому можливість контакту з абонентами за межами цієї групи звичайно надається в якості факультативної операції.

Транкінговий телефон працює в режимі почергового спілкування, передбачає можливість селекторного зв'язку, при якому декілька абонентів можуть спілкуватись один з одним одночасно. За допомогою транкінга можна передавати цифрову інформацію, включаючи шифрування повідомлень, Уже сьогодні можлива пряма передача повідомлень з абонентської радіостанції до комп'ютера. Транкінговий зв'язок, хоч значно дешевший і забезпечує практично всі послуги сотового зв'язку, проте має суттєвий недолік - телефон працює в напівдуплексному режимі, тобто в режимі почергового спілкування. Транкінгова система дозволяє здійснювати селекторний зв'язок, а також мати «пріоритетних» абонентів яким радіоканал надається за першою вимогою. Система сама веде документальний і статистичний облік своєї роботи. Транкінг підтримує усі види викликів - з абонентської станції в телефонну мережу, з однієї абонентської станції на іншу, з телефонної мережі на абонентську станцію, а також режим звичайного радіозв'язку між абонентами поза зоною обслуговування системи. Абонент транкінгової системи користується, за своїм вибором, автомобільною або ручною радіостанцією.

- Сотові телефони.

Особливістю цього виду зв'язку є автоматична передача підтримки рухомого абонента від одної бази станції до іншої при зміні якості сигналу, Найбільш дорогий і зручний - сотовий радіозв'язок, який забезпечує практично весь спектр послуг «звичайного» телефону. Якщо базові радіостанції «накривають» якусь площу повністю, то в будь-якій точці цієї території сотовий телефон забезпечує надійний зв'язок абонентів. Головна превага сотового зв'язку полягає в тому, що абонентський номер телефону «мандрує» з користувачем практично по всій території.

Технічні засоби управління. Неможливо уявити собі сучасну компанію, яка не застосовує у своїй повсякденній роботі засоби автоматизації офісу. Комп'ютери і оргтехніка не тільки докорінно змінюють вигляд організацій, стиль роботи, а й забезпечують велику мобільність і ефективність їх діяльності.

Велика кількість усіляких компонентів комп'ютерних комплексів, що пропонуються на ринку, створює значні проблеми в їх правильному застосуванні й інтегруванні.

Комплекс з офісного обладнання повинен бути не тільки технічно сучасним, а й оптимальним за складом, чітко орієнтованим на вирішення різноманітних завдань і підкріпленим могутньою сервісною підтримкою.

За останні десятиліття було створено декілька типів комп'ютерів: від маленьких, котрі можуть вміститись в долоні, до надзвичайно швидких суперкомп'ютерів. За швидкістю обробки сучасні комп'ютери можна згрупувати в класи: мікрокомп'ютери, робочі станції, міні-комп'ютери, великі ЕОМ і суперкомп'ютери.

Копіювальна техніка. Існує безліч класифікацій копіювальних апаратів залежно від різних параметрів. Існуюча нині копіювальна техніка ділиться на п'ять основних груп:

портативні копіювальні апарати, низько швидкісні машини, офісні копіри середнього класу, копіри для робочих і спеціальні копіювальні апарати.

Призначення копіювальної техніки - це обслуговування потреб великих офісів і бізнес-центрів, великі об'єми копіювання, необхідність брошурування і сортування документів, розподіл ресурсів і програмування великих об'ємів складних копіювальних робіт.

Принтери. Принтери - найбільш масове сімейство комп'ютерної периферії, яке за чисельністю у багато разів перевищує всі інші периферійні пристрої.

Споживачі властивості принтерів вдалося різко підвищити з початком періоду становлення матричних пристроїв, котрі підтримували різноманітні шрифти й алфавіти, а також графічний редактор. Нині для монохромного друку випускаються , в основному, принтери таких типів:

- матричні голчаті;
- принтери термодруку;
- струменеві;
- лазерні і світлодіодні.

Сканери. Сканером називається пристрій, який дозволяє вводити в комп'ютер двомірне зображення.

Переважна більшість сканерів використовується для підготовки і видання різних інформаційних матеріалів. Прогнозується широке застосування сканерів у сфері факсимільного зв'язку.

При роботі сканера відбувається такий процес. Як і фотокопіювальний пристрій, сканер освітлює оригінал, а його світлочутливий датчик із певною частотою вимірює інтенсивність відображеного оригіналом світла. Роздільна здатність сканера прямо пропорційна частоті вимірів. У процесі сканування пристрій перетворює величину інтенсивності у двійковий код, який передається в пам'ять ПЕОМ для подальшої обробки.

Відповідно до функціональних можливостей пристрою сканери поділяються на настільні, портативні і кольорові.

При виборі конкретного програмного забезпечення для сканера рекомендується брати до уваги такі характеристики:

- наявність механізму попереднього сканування, який забезпечує можливість виконання однократного сканування всієї сторінки з подальшим вибором дільниць меншого розміру для закінчення сканування;
- можливість встановлення широкого діапазону дозволів, що дозволяє обирати необхідну для кожного конкретного випадку величину. Як правило, це важливо при роботі з фотографіями і графікою;
- можливість регулювати контрастності і яскравості;
- можливість редагувати зображень;
- можливість створення файлів, формат яких відповідає іншим пакетам, що використовуються в системі.

Засоби збереження і резервування інформації. При експлуатації комп'ютера через різні причини можливі псування або втрата інформації на магнітних носіях. Це може статися через фізичне псування магнітного диска, неправильне коригування або випадкове знищення файлів, руйнування інформації комп'ютерними вірусами тощо. Щоби зменшити втрати або уникнути їх, потрібно мати копії файлів, що використовуються, і періодично оновлювати копії змінних робочих файлів.

Використовувати дискети з метою збереження інформації не раціонально і не зручно, в зв'язку з їх обмеженою місткістю. Доцільно застосовувати накопичувачі, що забезпечують порівняно невеликий час доступу і володіють великою місткістю. Використовуються для цього лазерні диски , накопичувачі на магнітооптичних дисках.

Сучасна інформаційна технологія.

Останні досягнення у сфері інформаційної технології можуть сприяти

вдосконаленню обміну інформацією в організаціях. Персональний комп'ютер уже зробив великий вплив на інформацію, котру керівники, допоміжний персонал і робітники розсилають й отримують. Електронна пошта дає робітникам можливість направляти письмові повідомлення будь-якій людині в організації. Це повинно зменшити традиційно невичерпний потік телефонних розмов. Крім того електронна пошта ефективний засіб зв'язку між людьми, що знаходяться в різних конторах , різних містах і, навіть, у різних штатам і країнах. Останні нововведення в системах телефонного зв'язку дозволяють одній людині направити кілька повідомлень, а після цього подзвонити й отримати відповідні та вихідні повідомлення.

Теми рефератів:

1. Технічне забезпечення комунікаційних процесів.
2. Апаратно-програмне забезпечення інформаційних зв'язків в організації.

Література: (8, 13, 14, 38, 52)

Питання 7. **Організаційно-технічні та режимні заходи безпеки інформаційних зв'язків.**

Вивчаючи це питання, студент має усвідомити, що бурхливий розвиток інформаційних технологій, комунікаційних мереж, засобів зв'язку та доступу до різноманітної інформації, що дозволив не тільки швидко обробляти величезні банки інформації, змінювати структуру комунікації між людьми, а й відбився у сфері інформаційної безпеки та захисту інформації як об'єкта і предмета праці, важливого продукту певної послуги.

Зараз в світі відбувається величезне зростання обсягів інформації, знання диференціюється та спеціалізується, неминуче зростає сфера послуг, тому процес забезпечення інформаційної безпеки є об'єктивним і закономірним. Держави, в залежності від свого інтелектуального, наукового, технологічного рівня розвитку мають різні перспективи щодо цього. Високорозвинуті держави світу вже пройшли початковий етап становлення суспільства інформаційної демократії, інші знаходяться на заключній фазі індустріалізму.

Українське законодавство в сфері інформаційних правовідносин, тобто суспільних відносин щодо володіння, користування і розпорядження інформацією, має не високий загальний рівень розробленості.

Державою визнано право власності на інформацію. Тому відповідно до ст. 41 «Конституції» інформація є предметом державної охорони, яка забезпечується Законом «Про інформацію» від 02.10.92р., Законом «Про захист інформації в автоматизованих системах» та ст.. 198-1 кримінального кодексу.

Поява та швидкий розвиток глобальної мережі Інтернет теж сказалися на розвитку інформаційного суспільства та відкрили нові проблеми щодо збереження інформаційних ресурсів. Завдяки Мережі стираються кордони між державами, вона представляє зовсім новий тип суспільної комунікації, нову модель спілкування між суб'єктами світового співтовариства, відкриває нові горизонти інформаційного обміну в межах майже всього світу. В той же час, нестримуваний та багато в чому ентропійний, хаотичний розвиток Мережі визвав забагато побоювань, поставив актуальні та серйозні питання щодо безпеки інформаційних зв'язків. Інтернет виступає саме як авангард інформаційного суспільства. Він повинен йому загрожувати, тому слід вирішувати ці питання, причому негайно. Все це породило цікаві та корисні дискусії щодо ролі, перспективах та загрозах Інтернет. Зараз пропонується багато теорій, концепцій щодо вирішення цих нагальних питань. Таким чином, становлення суспільства нового типу дуже гостро ставить питання інформаційної безпеки простору держави, людини, суспільства, відповідних інформаційних зв'язків. Це питання стає дуже актуальним і для нашої країни, отже, проблема інформаційної безпеки та захисту інформації нині має важливе значення.

Практичний досвід експлуатації комп'ютерних систем у провідних країнах показує,

що однією із основних потенційних загроз для інформації є так званий людський фактор – цілеспрямовані або випадкові деструктивні дії персоналу. (Вони становлять до 75% усіх випадків).

Дуже тривожним моментом у забезпеченні інформаційної безпеки громадян є "електронне стеження", тобто запис і прослуховування телефонних розмов, перлюстрація листів і інші методи поліцейського контролю. Таке спостереження можливо, і на робочих місцях, де виникає практика хронометрування всіх операцій і дій людини з точністю до тисячної частки секунди, його вільного часу, визначення міри придатності працівника, зарплати, здоров'я, кількості виробленої продукції, простою, відсутності через хворобу, професійної підготовки і т.д. За допомогою особливих програм комп'ютери можуть порівнювати й оцінювати працівників, підготовляти списки для чи звільнення, заохочення. Позитивне для підприємця обертається негативним для робітників та службовців.

Таким чином, особливості розвитку світу інформації, можливості необмеженого та неконтрольованого впливу, несанкціонований доступ (НСД), комп'ютерні віруси та т. ін. гостро поставили перед суспільством проблеми інформаційної безпеки, яка повинна здійснюватися комплексно та систематично з використанням різних засобів (апаратних, програмних та ін.) щоби запобігти інформаційному тиску та в цілому будь-якій іншій інформативній небезпеці.

Значущість і очевидна необхідність активного внутрішнього використання і активного розповсюдження інформації для забезпечення конкурентноздатності організації, важливість координації зусиль всіх спеціалістів, які рямо чи опосередковано залучені до сфери розробки і реалізації внутрішньої і зовнішньої комунікаційної політики організації потребують впровадження організаційно-технічних та режимних заходів з інформаційної безпеки.

Інформаційна безпека - стан, за якого забезпечується об'єктивне інформування суб'єктів підприємництва, гарантований захист їх інформаційних ресурсів та протидія негативному інформаційному впливу

Метою системи захисту інформації підприємства є:

- запобігання витоку, розкраданню, втрат, перекручування, підробки інформації;
- запобігання погроз безпеки особистості, підприємства, суспільства, держави;
- запобігання несанкціонованих дій по знищенню, модифікації, перекручуванню, копіюванню, блокуванню інформації;
- запобігання інших форм незаконного втручання в інформаційні ресурси і системи, забезпечення правового режиму документованої інформації як об'єкта власності;
- захист конституційних прав громадян на збереження особистої таємниці і конфіденційності персональних даних, що є в інформаційних системах;
- збереження, конфіденційності документованої інформації відповідно до законодавства.

Безпека інформації (information security) – стан інформації при якому забезпечується збереження визначених політикою безпеки властивостей інформації.

Сьогодні наявність механізмів захисту є однією з обов'язкових вимог при проектуванні автоматизованих систем обробки даних (АСОД), при чому не тільки спеціального призначення (військових, урядових і т.п.). Про масштаби цієї проблеми можна судити по тому, що велика кількість фірм спеціалізуються на проведенні робіт пов'язаних із захистом інформації: розробка і виробництво засобів захисту, консультування проектувальників, адміністраторів і користувачів АСОД, проектування, супровід і обслуговування механізмів захисту, їхня ревізія й ін.

Предметом захисту є дані, якими обмінюється людина з іншою людиною через ПЕОМ або із самої ПЕОМ.

Слід зазначити, що захисту підлягає лише та інформація, яка має визначену цінність, тобто та, володіння якою дозволяє її потенційному або реальному власнику

отримати будь-який виграш: моральний, матеріальний, політичний і ін. Оскільки в людському суспільстві завжди існують особи, які хочуть незаконним шляхом отримати інформацію, у власника виникає потреба в її захисті.

Цінність інформації є критерієм при прийнятті будь-якого рішення щодо її захисту.

Категорія важливості, як і цінність інформації, як правило, змінюються з часом і залежать від відношення до неї різних груп користувачів і потенційних порушників.

Рівень таємності - це адміністративна чи законодавча міра, яка визначає відповідальність особи за втрату або витік інформації. Вона регламентується спеціальними документами, по обліку державних, комерційних, службових або особистих інтересів.

Впливи на інформацію і незаконний доступ до неї розділяються на випадкові і зловмисні. Наслідки, до яких приводить реалізація погроз:

- знищення (втрата) інформації;
- модифікація інформації;
- витік інформації, ознайомлення з нею сторонніх осіб.

Основною метою створення системи захисту інформації є попередження наведених наслідків в інформаційній системі обробки даних (ООД).

Існують наступні методи її захисту від несанкціонованого доступу (НСД):

- обмеження доступу;
- розмежування доступу;
- розподіл доступу;
- криптографічне перетворення інформації;
- контроль і облік доступу;
- законодавчі заходи.

Зі збільшенням обсягів інформації, кількості користувачів, видів випадкових впливів, збільшується ймовірність зловмисного НСД до інформації. У зв'язку з цим розвиваються старі і виникають нові додаткові методи захисту інформації:

- методи функціонального контролю, що забезпечують діагностику і визначення збоїв апаратури, помилок людини, програмних помилок;
- методи підвищення вірогідності інформації;
- методи захисту інформації від аварійних ситуацій;
- методи контролю доступу до внутрішнього монтажу апаратури, лініям зв'язку і технічних органів управління;
- методи розмежування і контролю доступу;
- методи аутентифікації користувачів, технічних засобів, носіїв інформації, документів;
- методи захисту від побічного випромінювання і наведень.

Таким чином, проблема захисту інформації стає все більш актуальною. Аспекти проблеми є предметом інтенсивного обговорення на форумах фахівців з обчислювальної техніки і програмування, спеціально присвячених безпеці інформації в локальній і глобальній інформаційній мережах.

Захист інформації - комплекс заходів спрямованих на недопущення несанкціонованого доступу до носіїв інформації, її неконтрольованого поширення чи використання.

Інформаційна безпека - стан, за якого забезпечується об'єктивне інформування суб'єктів підприємництва, гарантований захист їх інформаційних ресурсів та протидія негативному інформаційному впливу.

Цілями системи захисту інформації підприємства є:

- запобігання витоку, розкрадання, утрати, перекручування, підробки інформації;
- запобігання погроз безпеки особистості, підприємства, суспільства, держави;
- запобігання несанкціонованих дій по знищенню, модифікації, перекручуванню, копіюванню, блокуванню інформації;

- запобігання інших форм незаконного втручання в інформаційні ресурси і системи, забезпечення правового режиму документованої інформації як об'єкта власності;
- захист конституційних прав громадян на збереження особистої таємниці і конфіденційності персональних даних, що маються в інформаційних системах;
- збереження, конфіденційності документованої інформації відповідно до законодавства.

Теми рефератів:

1. Технічне забезпечення безпеки інформаційних зв'язків в організації
2. Види режимів доступу до інформації.
3. Обмеження доступу як вид режиму доступу до інформації.
4. Розмежування доступу як вид режиму доступу до інформації.
5. Розподіл доступу як вид режиму доступу до інформації.
6. Криптографічне перетворення інформації.
7. Контроль і облік доступу до інформації.
8. Законодавче забезпечення режиму доступу до інформації.

Література: (1, 2, 9, 10, 12 ,19, 24, 39, 45, 51, 52).

Питання 8

Дотримання службової і державної таємниці у процесі реалізації інформаційних зв'язків. Стандарти захисту.

Як стверджують аналітики сьогодні проблеми і задачі великих компаній можуть бути порівнянні з проблемами і задачами цілих держав. Як і держави, вони співробітничають і воюють. Але війни тут звуться інформаційними: хто має інформацію, володіє якщо не світом, то фінансовими потоками. У зв'язку з цим дотримання режимів в їх діяльності набуває особливої ваги.

Проте, як не дивно, навіть сьогодні не всі керівники усвідомлюють нагальну потребу створення на їх підприємстві системи захисту комерційної таємниці. З числа тих, хто таку необхідність усе-таки розуміє, досить багато хто не знають, що варто робити, щоб зберегти ті або інші дані в таємниці, з вигодою реалізувати їх, не понести збитки від їх витоку або втрати. Деякі йдуть тільки по шляху оснащення підприємства технічними засобами захисту, цілком ігноруючи організаційно-правові методи. Мається на увазі, зокрема, створення нормативно-правової бази, прийняття і строге дотримання якої дозволить фірмі не тільки зберегти і використовувати з вигодою свої секрети, але у випадку витоку інформації з'явиться підставою для подачі позовної заяви.

В попередньому матеріалі йшлося, що тільки комплексна система може гарантувати досягнення максимальної ефективності захисту інформації, тому що системність забезпечує необхідні складові захисту і встановлює між ними логічний і технологічний зв'язок, а комплексність, що вимагає повноти цих складових, всебічне охоплення питань захисту, забезпечує її надійність**.**

Засоби захисту інформації. Засоби захисту інформації обираються відповідно до змісту таких структурних елементів моделі інформаційної безпеки підприємства:

1. Об'єкти злочинних посягань:

- технологічний процес опрацювання, передачі та зберігання
- інформації; інформаційні ресурси.

2. Перелік загроз:

- порушення термінів і порядку проходження документів;
- викривлення, фальсифікація, переадресування, несанкціоноване знищення, неправдива авторизація документів та повідомлень, які зберігаються у системі;
- порушення конфіденційності інформації, яка віднесена до комерційної таємниці.

3. Можливі суб'єкти, що здійснюють злочинні посягання:

- співробітник підприємства, який має повноваження доступу до інформаційної системи підприємства;
- співробітник підприємства, який не має повноважень доступу до інформаційної системи підприємства;
- особа, яка не є співробітником підприємства і не має повноважень доступу до інформаційної системи.

4. Можливі типи структурних посягань у інформаційній системі підприємства:

- втручання у технологічний процес опрацювання, зберігання і передавання інформації з метою реалізації злочинного посягання;
- використання санкціонованого користувача для втручання у технологічний процес опрацювання, зберігання і передавання інформації з метою реалізації злочинного посягання.

5. Форми здійснення злочинних посягань:

- змова, яка включає співробітника (співробітників) підприємства як учасника;
- використання співробітника (співробітників) підприємства без їхнього відома;
- здійснення економічного, фізичного або морального тиску на співробітника (співробітників) підприємства;
- імітація із злочинною метою дій санкціонованого користувача, який знаходиться на території підприємства;
- імітація із злочинною метою дій санкціонованого користувача, який знаходиться поза територією підприємства.

6. Група ризику санкціонованих користувачів:

- співробітники підприємства, що задіяні у технологічних процесах опрацювання, передавання і зберігання інформації;
- співробітники підприємства, що не задіяні у технологічних процесах опрацювання, передавання і зберігання інформації, але мають можливість організувати втручання у технологічний процес;
- співробітники організацій, з якими підприємство взаємодіє у процесах обміну інформацією, або співробітник організацій, які є для підприємства виконавцями робіт за угодами на тимчасовій або постійній основі.

7. Група ризику несанкціонованих користувачів:

- співробітники підприємства, які мають можливість здійснювати економічний, фінансовий або моральний впливу на санкціонованих користувачів інформаційної системи з метою реалізації злочинного посягання у інформаційній сфері;
- колишні співробітники підприємства або співробітники організацій, які взаємодіють з підприємством, які раніш мали доступ до інформаційної системи;
- злочинні елементи.

8. Мотиви злочинних посягань:

- економічний;
- емоційний (акт особистої помсти, образа та ін..);
- політичний (з метою завдання шкоди національній системі або країні у цілому).

9. Можливі місця здійснення злочинних посягань: будівлі, приміщення, технічні засоби (обчислювальна техніка, телекомунікаційне обладнання, канали зв'язку, програмні засоби).

Стандарти захисту інформації. Глобалізація комп'ютерних мереж створила для бізнес-діяльності не тільки відомі зручності та переваги, а й чимало проблем. Ідеться як про прямі крадіжки, вандалізм так, що особливо небезпечно, про зовнішнє підключення до комп'ютерної мережі установи. Нерідко їх працівники через можлиість доступу до інформаційних систем, здійснюють подібні операції (переказ грошей на приватні банківські рахунки); вносять цільові програми "вірусних нападів". Мають місце, також прості людські помилки операторів під час використання програм у поза контурних

комп'ютерних системах. В цілому, через таку інформаційну вразливість втрати, наприклад, західних компаній щорічно сягають сотень мільярдів доларів.

Британський інститут стандартів (BSI) і Міжнародна організація із стандартизації (ISO) за підтримки комерційних організацій, серед яких Shell, National Westminster Bank , Midland Bank, Unilever, British Telecom, Marks & Spenser, Logical та інші, розробили та впровадили стандарти інформаційної безпеки BS7799 та ISO17799. Вони, разом із такими загальновідомими міжнародними стандартами, як ISO9000, ISO14001, OHSAS18001, AS9100, здобули широке визнання у світі. Зазначені стандарти, узагальнивши найпередовіші досягнення в організації інформаційної безпеки підприємства чи організації, стали нормою взаємовідносин між діловими партнерами.

Тому перед комерційними та державними господарськими структурами сьогодні постало важливе завдання: не тільки забезпечити надійний захист інформації, а й організувати доступ до даних і ефективну роботу з ними. Стандарти BS7799 та ISO17799 визначають загальну організацію, класифікацію даних, системи доступу, напрями планування, відповідальність співробітників, використання оцінки ризику тощо в контексті інформаційної безпеки. Стандарти передовсім призначені для економії фінансових витрат фірм, а у деяких випадках навіть запобіганню банкрутства, і не є зовнішньою обов'язковою вимогою, що призводить до додаткової статті витрат фірм.

BS7799 та ISO17799 містять понад 100 елементів управління інформаційною безпекою, що об'єднані в такі групи:

1. Політика в галузі безпеки. Мета: забезпечити чітке управління та підтримку політики у сфері інформаційної безпеки з боку керівництва фірми.
2. Організація системи безпеки. Мета: створити організаційну структуру, яка впроваджуватиме та забезпечуватиме працездатність системи інформаційної безпеки в організації.
3. Класифікація ресурсів та управління. Мета: підтримувати адекватну інформаційну безпеку організації шляхом покладання персональної відповідальності, а також класифікації інформаційних ресурсів за необхідністю і пріоритетами захисту.
4. Безпека та персонал. Мета: зменшити ризик людських помилок, розкрадань та неправильного використання обладнання, у тому числі шляхом ефективного навчання персоналу та впровадження механізму запобігання інцидентам.
5. Фізична та зовнішня безпека. Мета: убезпечити від несанкціонованого доступу, пошкодження та погіршення роботи інформаційної системи фірми.
6. Управління робочими станціями та мережами. Мета: налагодити безпечне функціонування комп'ютерів та мереж.
7. Контроль доступу до системи. Мета: управляти доступом до ділової інформації, унеможливлювати несанкціонований доступ та викривати нелегальну діяльність.
8. Розробка та обслуговування системи. Мета: дотримуватися вимог безпеки під час створення або розвитку інформаційної системи фірми, підтримувати безпеку додатків, периферії та даних.
9. Забезпечення безперервної роботи. Мета: підготувати план дій для його застосування в разі надзвичайних обставин, аби не порушити безперервну діяльність організації.
10. Відповідність законодавству. Мета: забезпечити виконання вимог відповідного громадянського та кримінального законодавства, у т. ч. законів про авторські права і захист інформації.

Така структура дозволяє вибирати методи управління, прийнятні для конкретної фірми або сфери відповідальності всередині організації. Крім того, окремо виділяється 10 так званих ключових елементів управління, що є фундаментальними і стосуються всіх організацій за будь-яких умов. Це:

1. Політика з інформаційної безпеки.
2. Поділ відповідальності за дотримання інформаційної безпеки.

3. Освіта та тренінг з питань інформаційної безпеки.
4. Звітність за інцидентами, пов'язаними з порушенням безпеки.
5. Захист від вірусів.
6. Забезпечення безперервності роботи.
7. Контроль за копіюванням ліцензованого програмного забезпечення.
8. Захист архівної документації фірми.
9. Захист персональних даних.

Ризики та загрози визначають набір послуг, які надають фірми з інформаційної безпеки. Замовник та виконавець складають так звані функціональні профілі захисту інформації (набори послуг) у вигляді спеціальних нормативних документів, яким надається ім'я та числовий ідентифікатор. До уваги беруться насамперед умови функціонування організації, її спеціалізація, особливості ринкового оточення і завдань середньо- та довгострокової стратегії бізнесу. Головне, щоб у результаті подібного аналізу став можливим реальний та ефективний вибір послуг з "меню" BS7799 та ISO17799 відповідно до компонентів єдиних критеріїв, що оформлюється у вигляді Декларації з використання.

Однією з особливостей сьогодення в галузі захисту інформації є інтернаціоналізація стандартизації. Гипершвидкий розвиток інформаційних технологій, формування всесвітнього інформаційного простору, надто поступова інтеграція до нього України є незаперечними фактами. Створення адекватних і надійних систем захисту інформації в таких умовах не під силу одній країні. Тому необхідно вивчати та використовувати міжнародний практичний досвід, визнані методологічні підходи для впровадження їх у вітчизняну ринкову реальність. Слід адаптувати та розробити нові нормативні документи, які повинні відповідати міжнародним стандартам.

Прогнозується, що наступні 10 років в Україні будуть періодом стрімкого зростання попиту на сертифікацію за стандартами B87799 та 18017799, оскільки темпи росту електронної комерції значно випереджатимуть темпи росту інших секторів та сегментів ринку. Одночасно чималий інтерес до сертифікації виявлятимуть такі сфери комерційної і державної діяльності, як банки, фінансові та страхові компанії, торговельні та туристичні фірми, телекомунікаційні структури, державні податкові органи та органи внутрішніх справ, медичні заклади, підприємства транспорту і т. п. Швидкий розвиток B87799 та значний інтерес до нього свідчать про те, що в найближчій перспективі відповідність новому стандарту інформаційної безпеки стане важливою умовою комерційного успіху.

Теми реферату:

1. Канали поширення інформації в процесі реалізації інформаційних зв’язків.
2. Характеристика джерел цінної підприємницької інформації.
3. Основні напрямки захисту службової інформації і документації.
4. Система захисту цінної інформації: поняття, структура, технологія.
5. Основні елементи службової і державної таємниці та захисту інформації.

Література: (1, 16, 26, 28, 31, 34, 36, 50)

Питання 9. **Організація діяльності по захисту документної інформації на підприємстві (організації, фірмі).**

1. Склад та спрямування захисту документної інформації.
2. Система захисту цінної інформації і конфіденційних документів.
3. Технологія захисту документної інформації.
4. Порядок роботи персоналу з конфіденційними документами.

В попередніх матеріалах зазначалось, що в менеджменті найважливішу роль відіграє документ.

1. Склад та спрямування захисту документної інформації.

Для документування інформації підприємця, яка є результатом творчої інтелектуальної праці в науці та виробництві, найбільш характерні не текстові, а зображувальні способи. Досить часто конфіденційна інформація документується фотографічними, відеографічними та іншими способами. Цінність інформації може бути кошторисною категорією і відображати конкретний розмір прибутку при її використанні чи розмір збитків при її втраті. Інформація стає часто цінною через її правове значення для організації чи розвитку бізнесу, наприклад, установчі документи, програми та плани, договори з партнерами та посередниками і т. і. Цінність може відображати її перспективне, наукове, технічне чи технологічне значення. Отже, власна цінна інформація підприємця не обов'язково є конфіденційною. Часто звичайний правовий документ важливо зберегти в цілісності та безпеці від викрадача чи стихійного лиха. Цінну конфіденційну ділову інформацію, як правило, містять: плани розвитку виробництва; ділові плани; плани маркетингу, бізнес-плани; списки власників акцій та інші документи. Найбільш цінні відомості про виробництво і продукцію, ринок, наукові розробки, матеріально-технічне забезпечення, умови контрактних переговорів, відомості про персонал, принципи управління фірмою, систему безпеки фірми і ті.

Комерційна цінність інформації, як правило, недовготривала і визначається часом, необхідним конкуренту для створення тієї ж ідеї чи її викрадення та відтворення, опублікування та переходу до числа загальновідомих. Ступінь цінності інформації та необхідна надійність її захисту знаходяться в прямій залежності. Зарубіжні фірми з метою підвищення свого престижу та конкурентноздатності товарів часто використовують різні рекламні прийоми і, зокрема, створюють неіснуючі секрети. Такий "секрет" вміло розголошується зважаючи на загальновідому істину підслуханому вірять більше, ніж почутому. Виявлення та регламентація реального складу інформації, що представляє цінність для підприємця і належить захисту, є основоположною частиною системи захисту.

Склад цінної інформації визначається її власником і фіксується в спеціальному переліку. Перелік цінних відомостей, що складають таємницю фірми, є постійним робочим матеріалом керівництва фірми, служб безпеки та конфіденційної документації Він регулярно оновлюється, коректується та *являє собою інвентарний список відомостей про конкретні роботи, конкретну продукцію, конкретні дослідження, конкретні контракти* і т.і. В перелік включаються дійсно цінні відомості ("ізюминки") про кожну роботу фірми, хоча певна номенклатура типових відомостей в переліку може міститися. В кожній позиції переліку *рекомендується вказувати гриф конфіденційності* відомостей, прізвища співробітників, які мають право доступу до них і які несуть відповідальність за їх зберігання, термін дії грифу або найменування події, яка знімає це обмеження, види документів та баз даних, в яких ці відомості фіксуються і зберігаються.

Під конфіденційним (закритим) документом, тобто документом, до якого обмежений доступ персоналу, треба розуміти необхідним чином оформлений носій цінної задокументованої інформації, яка складає інтелектуальну власність підприємця.

Особливість конфіденційного документу в тому, що він представляє собою одночасно: масовий носій захищеної інформації, основне джерело накопичення та розповсюдження цієї інформації, в тому числі її розголошення (витоку), і обов'язковий об'єкт захисту. Конфіденційний характер включеної в документ інформації позначається *грифом обмеження доступу* до документа, який ініціює виділеній; його з загального потоку і обробку в спеціальному автономному режимі, а також поширює на документ захисні та інші міри підвищеної уваги та контролю. Гриф обмеження доступу до документа або гриф конфіденційності представляє собою службову відмітку (реквізит), яка проставляється на носії інформації чи супровідному документі.

Інформація і документи, віднесені до підприємницької таємниці, мають декілька рівнів грифів обмеження доступу, відповідних різним степеням конфіденційності інформації: перший, самий низький і масовий рівень - грифи "Комерційна таємниця", "Конфіденційно", "Конфіденційна інформація"; другий рівень - "Комерційна таємниця. Строго конфіденційно", "Строго конфіденційно", "Строго конфіденційна інформація",

"Конфіденційно - Особливий контроль". В практичній діяльності може використовуватися також однорівнева система грифування (грифів тільки першого рівня) або інколи - трьохрівнева, при якій вводиться вищий по значенню гриф – «Комерційна таємниця особливої важливості".

Отже, будь-яка підприємницька діяльність завжди пов'язана із створенням, використання та зберіганням значних об'ємів інформації та документів, що представляють певну цінність для фірми які належать обов'язковому захисту від різного виду погроз. З цією метою на носії інформації позначається гриф обмеження доступу, який відносить цей носій до категорії захищених конфіденційних документів і ініціює включення по відношенню до нього системи захисних заходів.

2. Система захисту цінної інформації і конфіденційних документів. *Система захисту інформації* (СЗІ) представляє собою комплекс організаційних, технічних і технологічних засобів, методів і мір, які перешкоджають несанкціонованому (незаконному) доступу до інформації. Власник інформації особисто визначає не тільки склад цінної інформації, яка належить захисту, але й відповідні способи та засоби захисту. Одночасно ним розробляються міри матеріального і морального стимулювання співробітників, які дотримуються порядку захисту цінної інформації, і міри відповідальності персоналу за розголошення таємниці фірми. Система захисту інформації повинна бути багаторівневою з ієрархічним доступом до інформації, гранично конкретизованою і прив'язаною до специфіки фірми по структурі методів та засобів захисту, що використовуються, відкритою для регулярного оновлення, надійної як в звичайних, так і в екстремальних ситуаціях. Вона не повинна створювати співробітникам фірми серйозні незручності в роботі. Комплексність системи захисту досягається її формуванням з різних елементів -правових, організаційних, технічних та програмно-математичних. Співвідношення елементів та їх зміст забезпечують індивідуальність системи захисту інформації фірми і гарантують її неповторність та трудність подолання.

Конкретну систему захисту можна уявити у вигляді цегляної стіни, як складається з безлічі різноманітних елементів (цегли). Співвідношення елементів системи, їх склад та взаємозв'язок відображають, визначають не тільки її індивідуальність, але й конкретний заданий рівень захисту з врахуванням цінності інформації та вартості подібної системи. Елемент правового захисту інформації передбачає: наявність в засновницькій та організаційних документах фірми, контрактах, що укладаються із співробітниками, і в посадових інструкціях положень та зобов'язань по захисту відомостей, що складають таємницю фірми і її партнерів, формулювання і доведення до відома всіх співробітників фірми механізму правової відповідальності за розголошення конфіденційних відомостей. В правовий елемент системи захисту може також включатись страхування цінної інформації від різних ризиків.

Елемент організаційного захисту інформації містить міри управлінського та обмежувального характеру, які спонукають персонал дотримуватися правил захисту конфіденційної інформації і включає в себе:

- формування і регламентацію діяльності служби безпеки фірми, забезпечення цієї служби нормативно-методичними документами по організації і технології захисту інформації;
- регламентацію та регулярне оновлення переліку (списку) цінної, конфіденційної інформації, яка підлягає захисту, складання і ведення переліку конфіденційних документів фірми;
- регламентацію системи (ієрархічної схеми) обмеження доступу персоналу до конфіденційної інформації;
- регламентацію технології захисту і обробки конфіденційних документів фірми;
- побудова захищеного традиційного або без паперового документообігу;
- побудова технології документування цінної інформації, складання, оформлення, виготовлення і видавництва конфіденційних документів;
- побудова технологічної системи обробки і збереження конфіденційних документів;
- організацію архівного зберігання конфіденційних документів;

- регламентацію захисту цінної інформації фірми від несанкціонованих дій персоналу; порядок і правила роботи персоналу з конфіденційними документами і інформацією, контроль за виконанням всіма співробітниками цього порядку і правил;
- відбір персоналу для роботи з конфіденційною інформацією, навчання та інструктування співробітників;
- порядок захисту інформації при веденні переговорів, проведенні нарад по конфіденційним питанням, прийомі відвідувачів, здійснення рекламної, виставочної та іншої діяльності;
- регламентацію аналітичної роботи по виявленню загроз цінній інформації фірми і каналів витоку інформації;
- обладнання і атестацію приміщень і робочих зон, виділених для здійснення конфіденційної діяльності, ліцензування технічних систем і засобів захисту інформації та охорони;
- регламентацію пропускного режиму на території, в будівлях і приміщеннях фірми, ідентифікацію персоналу та вантажу;
- регламентацію системи охорони території, будівлі, приміщень, обладнання, грошових засобів, транспорту і персоналу фірми;
- регламентацію організаційних питань експлуатації технічних засобів захисту інформації і охорони;
- регламентацію дій служби безпеки і персоналу в екстремальних ситуаціях;
- регламентацію роботи по управлінню системою захисту інформації фірми.

Елемент організаційного захисту є стріжнем, який зв'язує в одну систему всі інші елементи. Центральною проблемою при розробці методів організаційного захисту інформації є формування дозвільної (обмежувальної) систем і доступу персоналу до конфіденційних відомостей, документів і баз даних. Важливо чітко і однозначно встановити: хто, кого, до яких, відомостей, коли, на який період і як допускає.

Дозвіл (санкція) на доступ до цих відомостей завжди є строго персоніфікованим і видається керівником в письмовому вигляді: наказом, що затверджує схему посадового чи іменного доступу до інформації, резолюцією на документі, списком-дозволом в карточці видачі справи або на обложці справи ознайомлення з документом.

Організаційні міри захисту відображаються в нормативно-методичних документах служби безпеки фірми. У зв'язку з цим часто використовується єдина назва двох розглянутих вище елементів системи захисту - елемент організаційно-правового захисту інформації. Елемент *технічного захисту* включає: засоби захисту технічних каналів витоку інформації, що виникають під час роботи ЕОМ, засобів зв'язку, копіювальних апаратів, принтерів, факсів та інших приладів і обладнання; засоби захисту приміщень від візуальних та акустичних способів технічної розвідки; засоби охорони будівель і приміщень від проникнення сторонніх осіб (засоби спостереження, сповіщення, сигналізації, інформування і ідентифікації, інженерні споруди); засоби протипожежної охорони; засоби виявлення приладів і пристроїв технічної розвідки (підслуховувальних та передавальних пристроїв, звукозаписувальної та телевізійної апаратури і т.д.). *Елемент програмно-математичного захисту інформації* включає: регламентацію доступу до електронних документів персональними паролями, що ідентифікуються командами та іншими найпростішими методами захисту; регламентацію спеціальних засобів і продуктів програмного захисту; регламентацію криптографічних методів засобів захисту інформації в ЕОМ та мережах, криптографування (шифрування) тексту під час передачі їх по каналам звичайного та факсимільного зв'язку, під час пересилки поштою. В кожному елементі захисту можуть бути реалізовані на практиці тільки окремі складові частини. Наприклад, в організаційному захисті можна регламентувати тільки прийоми обробки конфіденційних документів і систему доступу до них персоналу.

Методи і засоби захисту інформації в рамках системи захисту *повинні регулярно* змінюватись з метою попередження їх розкриття зловмисником. Конкретна система захисту інформації фірмі завжди є строго конфіденційною. Спеціалісти, які розробляли що систему, ніколи не повинні бути її користувачами. Отже, система захисту конфіденційної інформації, яка

використовується фірмою, є індивідуалізованою сукупністю необхідних елементів захисту, кожний з яких окремо вирішує свої специфічні для даної фірми задачі і володіє конкретизованим відносно цих задач змістом. В комплексі ці елементи формують багато граничний захист секретів фірми і дають відносну гарантію безпеки підприємницької діяльності фірми.

3. Технологія захисту документної інформації. *Документообіг* як об'єкт захисту представляє собою сукупність (мережу) каналів розповсюдження документованої конфіденційної інформації по споживачам у процесі управлінської та виробничої діяльності. *Рух документованої інформації* не можна розпродати тільки як механічне переміщення документів по інстанціям, як функцію поштової доставки кореспонденції адресатам. Основною характеристикою такого руху є його технологічна комплексність, тобто з'єднання в єдине ціле управлінських, діловодних та поштових задач, що визначають в сукупності зміст переміщення документів. При русі документів (в тому числі електронних) по інстанціях створюються потенційні можливості втрати цієї інформації за рахунок розширення числа джерел, що володіють цінною інформацією.

Головним напрямом захисту документованої інформації (документів) від всіх видів загроз *є формування захищеного документообігу і використання в обробці і зберіганні документів* технологічної системи, що забезпечує безпеку інформації на любому типі носія. За рахунок цього досягається можливість контролю конфіденційної інформації в її джерелах і каналах розповсюдження. Окрім загальних для документообігу принципів захищений документообіг базується на ряді додаткових принципів персональної відповідальності співробітників за збереження носія і таємницю інформації; обмеженні ділової необхідності доступу персоналу до документів, справ і базам даних; операційному обліку документів і контролю за їх збереженням у процесі руху, розгляду, виконання і використання; жорсткій регламентації порядку роботи з документами, справами і базами даних для всіх категорій персоналу.

Однією з найважливіших вимог до захищеного документообігу є вибірковість у доставці і використання персоналом цінної інформації. Вибірковість призначена не тільки дня забезпечення оперативності в отримання користувачем цінної інформації, але й обмеження у доставці йому тієї інформації, робота з якою йому дозволена у відповідності з його функціональними обов'язками. В основі вибірковості в доставці і використанні конфіденційних документів лежить діюча у фірмі дозвільна (розмежувальна) система доступу персоналу до конфіденційної інформації, документам, справам і базам даних. Система в даному випадку передбачає цілеспрямоване дроблення конфіденційної інформації між співробітниками на складові елементи, кожний з яких окремо значної цінності не представляє. Захист документованої інформації в потоках досягається одночасним використанням як дозвільних (розмежувальних) мір, так і комплексом технологічних процедур і операцій, які входять в систему обробки і зберігання документів, що забезпечує розгляд, виконання, використання і рух документів.

Необхідно підкреслити, що технологічні системи обробки і зберігання конфіденційних і відкритих документів базуються на єдиній науковій і методичній основі. Вони єдині по структурі. Однак між ними спостерігаються деяка, різниця. Так, технологічна система обробки і зберігання відкритих документів (діловодна, автоматизована або змішана) призначена для вирішенні завдань в одній сфері - документаційного забезпечення управління. У свою чергу, технологічна система обробки і зберігання конфіденційній документів вирішує завдання не тільки у вказаній сфері, але й в сфері захисту інформації конфіденційних документів при роботі з ними персоналу. До цих завдань можна віднести наступні: попередження несанкціонованого доступу любої особи до документу, його частіш, варіантів, чорновиків, копій; забезпечення фізичного збереження документів і носіїв конфіденційної інформації; забезпечення збереження таємниці фірми, цінної інформації, яка міститься в документах. Крім того, технологічна система обробки і зберігання конфіденційних документів розповсюджується не тільки на управлінську (ділову) документацію, але й на конфіденційні конструкторські, технологічні, науково-технічні та інші подібні документи, документовану інформацію, записану на різних технічних носіях. Захист технічних носив

конфіденційної інформації (машиночитаючих документів) має важливе значення особливо на поза машинних стадіях їх обробки і зберігання. Саме на цих стадіях велика ймовірність втрати носія, його копіювання або знищення, підміни і фальсифікації.

Обробка і зберігання конфіденційних документів на різних стадіях їх руху має свої особливості. *Обробка документів, що надходять і відправляються*. В процесі обробки конфіденційних документів, вирішуються наступні задачі захисту інформації і її носіїв: не допустити попадання в дану фірму конфіденційних документів інших фірм і організацій; переконатися, що конверти, пакети з конфіденційними документами не відкривались на шляху проходження від відправника до адресата; попередні втрату документів після відкриття пакета; виключити можливість ознайомлення технічних робітників фірми з конфіденційними документами; виключити можливість ознайомлення любих працівників фірми з конфіденційними документами, які мають помітку "Особисто"; не допустити втрату документів і їх частин за рахунок неповного вилучення їх з конвертів; переконатися в комплектності документу, наявності всіх листів, примірників та інших частин, відсутності факту підміни документу. Пакети, конверти, які містять конфіденційні документи, надходять з поштового відділення зв'язку (цінні, заказні і прості відправлення), від кур'єрів установ і фірм, від відвідувачів. Ці документи можуть також приходити по факсимільному зв'язку, електронній пошті, по телеграфному і телетайпному зв'язку. Важкість виділення конфіденційних документів з загального потоку кореспонденції полягає в тому, що на пакетах, конвертах і часто на самих документах не ставиться гриф конфіденційності. Пояснюється це не тільки суто індивідуальним підходом до присвоєнім інформації статусу конфіденціальної, але й небажанням відправника звертати увагу сторонніх осіб на гриф обмеження доступу. Враховуючи цю особливість, відкриття документів, попередній розгляд і розподіл всієї кореспонденції, яка надходить, виконується кваліфікованим співробітником служби конфіденційної документації фірми, який добре знає структуру фірми, функції структурних підрозділів і співробітників, склад конфіденційної інформації Документи, що надходять по лініям факсимільного зв'язку, також продивляються цим співробітником з метою визначення можливої їх конфіденційності. Співробітник відкриває всі пакети, конверти, бандеролі (крім тих, що мають помітку "Особисто"), перевіряє правильність адресування та комплектність документів, веде облік конфіденційних документів і формування довідково-інформаційного банку даних по документам.

Облік конфіденційних документів передбачає не тільки реєстрацію факту створення (видання) або отримання документа, але й обов'язково фіксацію всік переміщень документа по інстанціях, керівникам і виконавцям у процесі розгляду, виконання і використання документів. Облік цих документів та їх зберігання завжди централізовані в підрозділі конфіденційної документації фірми або у референта першого керівника.

4. Порядок роботи персоналу з конфіденційними документами. При виході документів за межі служби конфіденційної документації їх безпека різко знижується за рахунок санкціонованого ознайомлення з ними значної кількості співробітників фірми. У зв'язку з цим правильна організація роботи персоналу з цими документами є дуже важливою. Особливо велика загроза електронним документам в результаті потенційної доступності інформації великій кількості співробітників і важкості визначення часто самого факту крадіжки інформації.

Керівники і виконавці фірми під час роботе з конфіденційними документами зобов'язані: знайомитися тільки з тими конфіденційними документами, до яких вони отримали дозвіл на доступ в силу посадових обов'язків; пред'являти працівнику служби конфіденційної документації документи, які за ним числяться, для перевірки їх наявності і комплектності; вести облік документів, які у них знаходяться; щодня по закінченні робочого дій перевіряти наявність документів, здавати їх на зберігання в службу конфіденційної документації; негайно повідомляти безпосередньому керівнику і в службу конфіденційної документації про втрату або недостачу документів, виявлення лишніх або неврахованих документів, окремих листів; здавати по опису в службу конфіденційної

документації всі документи, які за ними числяться, при звільненні, перед виходом у відпустку, від'їзді у відрядження.

Всі передачі конфіденційних документів керівникам і виконавцям повинні реєструватися в картках обліку документів. Прийом та видача документів здійснюються під розпис, що необхідно для встановлення факту покладення персональної відповідальності за документ на конкретних співробітників.

Керівники, виконуючи процедуру розгляду документів, вирішують наступні завдання захисту інформації: прийняття правильного рішення по складу виконавців, допущених до документу; виключення можливості ознайомлення з документом сторонніх осіб; попередження можливості крадіжки або копіювання документів відвідувачами, секретарем та іншими особами; виключення можливості витоку інформації по технічним каналам. При цьому необхідно пам'ятати, про сторонньою особою є люба особа, яка не має права доступу до даного конкретного документу, в тому числі інші керівники і спеціалісти фірми.

Співробітник служби конфіденційної документації, видаючи документи виконавцям для роботи, зобов'язаний: попередити видачу документа особі, яка не має права доступу до нього; зафіксувати факт передачі документу виконавцю; забезпечити фізичне зберігання документа, додатків, листів і інших частин документа; ознайомити виконавця тільки з тією частиною документа, яка йому адресована; попередити можливість ознайомлення з документом сторонньої особи при видачі документа виконавцю і поверненні документа; забезпечити облік документів, що знаходяться у виконавців.

Відповідальність за збереження конфіденційних документів і попередження витоку інформації в підрозділах фірми несуть їх керівники. Друкування конфіденційних документів на паперовому носії проводиться співробітником служби конфіденційної документації на друкарській машинці або за допомогою ПЕОМ. Виготовляти документи може й сам виконавець на своєму робочому місці при умові забезпечення збереження таємниці фірми. На останньому листі кожного примірника документу проставляється кількість надрукованих примірників, їх адреса або місцезнаходження, прізвище та номер телефону виконавця, прізвище оператора, що друкував документ, і дата.

Робота з електронними конфіденційними документами дозволяється тільки при наявності у фірмі сертифікованої системи захисту комп'ютера і локальної мережі. При роботі з конфіденційними документами керівники і виконавці повинні бути забезпечені постійним робочим місцем; особистим сейфом (металічною шафкою) і кейсом для зберігання документів; номерною особистою металевою печаткою. *Не дозволяється зберігання конфіденційних документів в ящиках робочого столу*, в шафах та інших широко доступних місцях, навіть якщо вони мають засуви. Якщо на робочому місці керівника або виконавця відсутні необхідні умови для роботи з конфіденційними документами, то ознайомлення з документами і їх виконання здійснюється у спеціальному приміщенні служби конфіденційної документації. Тут же ведеться й робота з документами особливої цінності.

Теми рефератів:

1. Документ як матеріальна форма фіксації інформації.
2. Документування конфіденційної інформації.
3. Перелік цінної інформації як робочий матеріал керівника: склад та характеристика.
4. Особливості конфіденційного документу.
5. Джерела конфіденційної документованої інформації.
6. Типологія загроз безпеці документної інформації.
7. Поняття та канали втрати (витіку) інформації.
8. Складові та характеристика системи захисту інформації (СЗІ).
9. Документообіг як об’єкт захисту конфіденційної інформації. Принципи захисту документообігу.
10. Вимоги до захищеності документообігу.

11. Облік конфіденційних документів.
12. Форми і методи перевірки наявності конфіденційних документів.
13. Основні правила організації роботи.

Література: (1, 2, 3, 7, 10, 12, 16, 24, 28)

Запитання та завдання для самоконтролю:

1. Збирання інформації як інформаційний процес та структура його інформаційних зв'язків.
2. Обробка інформації як інформаційний процес та зміст його інформаційних зв'язків.
3. Пошук інформації як інформаційний процес та особливості його інформаційних зв'язків.
4. Поширення інформації як інформаційний процес.
5. Інформаційне обслуговування, характеристика та види.
6. Документація та діловодство в організації як основа реалізації інформаційних зв'язків.
7. Документаційне забезпечення управління, характеристика та види.
8. Організаційно-розпорядча документація організації, характеристика та види.
9. Види інформаційних матеріалів з розкриття змісту документів.
10. Інформаційно-технологічний простір організації.
11. Інформаційні потоки в організації, характеристика та види.
12. Бар'єри на шляху інформаційних потоків в організації.
13. Заходи з удосконалення інформаційних зв'язків в організації.
14. Види інформаційних повідомлень.
15. Комунікаційні потреби організації.
16. Основні підходи до класифікації комунікацій.
17. Типи комунікацій.
18. Види комунікацій.
19. Визначення та характеристика інформаційних комунікацій.
20. Визначення комунікаційного процесу.
21. Інформаційні зв'язки в комунікаційному процесі.
22. Сучасні комунікаційні стратегії.
23. Основні методи поширення інформації про діяльність організації.
24. Етапи розробки плану комунікацій в організації.
25. Вибір засобу передачі повідомлення.
26. Технічне забезпечення комунікаційних процесів.
27. Апаратно-програмне забезпечення інформаційних зв'язків в організації.
28. Технічне забезпечення безпеки інформаційних зв'язків в організації.
29. Види режимів доступу до інформації.
30. Обмеження доступу як вид режиму доступу до інформації.
31. Розмежування доступу як вид режиму доступу до інформації.
32. Розподіл доступу як вид режиму доступу до інформації.
33. Криптографічне перетворення інформації.
34. Контроль і облік доступу до інформації.
35. Законодавче забезпечення режиму доступу до інформації.
36. Спрямування захисту документної інформації.
37. Захист цінної інформації.
38. Захист конфіденційних документів.
39. Документообіг як об'єкт захисту документованої інформації. Потенційні можливості втрат інформації.
40. Порядок роботи персоналу з конфіденційними документами.

Список літератури:

Основна

1. Антонюк А.О. Основи захисту інформації в автоматизованих системах: Навч. посіб.- К.: КМ Академія, 2003.- 244 с.
2. Башлы П.Н. Информационная безопасность.- Ростов н/Д: Феникс, 2006.- 253 с.
3. Бибик С.П., Сюта Г.М. Ділові документи та правові папери. – Х.: Фоліо, 2005. – 493 с
4. Герчикова И.Н. Менеджмент: Учеб. для вузов. – 4-е изд. перераб. и доп.; М.: ЮНИТИ –ДАНА, 2007. – 511 с.
5. Герчикова И.Н. Менеджмент: Практикум. Учеб. пособ. для студентов вузов. –М.: ЮНИТИ –ДАНА, 2005. – 799 с.
6. Горбаченко Т.Г. Аналітико-синтетична переробка документальної інформації: Навч. посіб.- К.: Ун-т Україна, 2005.- 236 с.
7. Домарєв В.В. Організація захисту інформації на об'єктах державної та підприємницької діяльності: Навч. посіб./ В.В.Домарєв, С.О.Скворцов.- К.: Вид-во Європ. ун-ту, 2006.- 102 с.
8. Информационные технологии управления: Учеб. пособ. для вузов. / Под ред. Г.А.Титаренко. - М.: ЮНИТИ –ДАНА, 2005. – 127с.
9. Компьютерные преступления: их предупреждение и выявление/ Захарченко В. Ю., Лазуренко В. И., Олифиров А. В. и др.- К.: ЦНЛ, 2007.- 170 с.
10. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посіб.- К.: Кондор, 2004.- 384 с.
11. Маслова В.М. Управление персоналом предприятия.: Учеб. пособ. - М.: ЮНИТИ – ДАНА, 2007. – 159 с.
12. Організаційно-правові основи захисту інформації з обмеженим доступом: Навч. посіб./ Ред. Сідак В С.- К.: Вид-во Європ. ун-ту, 2006.- 232 с.
13. Саак А.Э. Информационные технологии управления: Учеб./ А.Э.Саак, Е.В.Пахомов, В.Н.Тюшняков.- Спб.: Питер, 2005.- 320 с
14. Уткин В.Б., Балдин К.В. Информационные системы в экономике: Учеб. пособ. для вузов - М.:.- ЮНИТИ –ДАНА, 2005. - 335 с.

Додаткова

15. Арсеньев Ю.Н., Балдин К.В. Информационные системы и технологии. Экономика: Учеб. пособ. для вузов. – М.: ЮНИТИ – ДАНА, 2005.-335 с. Безмалый В.Ф. Атаки изнутри в корпоративной среде// Корпоративные системы.- 2005.- №4.- С.75-80.
16. Білик В.М. Інформаційні технології та системи: Навч. посіб./ В.М.Білик, В.С.Костирко.- К.: ЦНЛ, 2006.- 232 с.
17. Білоус В.С. Зв'язки з громадскістю (паблік рилейшнз) в економічній діяльності: Навч. посіб.- К.: КНЕУ, 2005.- 275 с.
18. Богуш В.М. Інформаційна безпека держави/ В.М.Богуш, О.К.Юдін.- К.: МК-Прес, 2005.- 432 с.
19. Бондар Ю. В. Проблеми інформаційної безпеки в умовах перехідного суспільства// Персонал.- 2003.- №8.- С.47-49.
20. Бондар Ю.В. Національний інформаційний простір новітньої України: становлення та функціонування у процесі політичної трансформації суспільства: Монографія.- К.: МАУП, 2007.- 184 с.
21. Бондаренко И.О., Дубницкий В.И. Менеджмент – корпоративный, маркетинг, информационный, антикризисный: Справ. информ. пособ. для специалистов, научн. работников и предпринимателей / Донецк. инст-т управления. – Донецк.: ООО «Юго-Восток ЛТД», 2004. - 140 с.
22. Ворошилов В.В. Современная пресс-служба.- Спб.: Изд-во Михайлова В.А., 2005.- 256 с.

23. Главатый В.К. Методы защиты информации/ В.К.Главатый, Н.А.Манохина// Корпоративные системы.- 2005.- №4.- С.65-69.
24. Горфинкель В.Я. Коммуникации и корпоративное управление.: Учеб. пособ. для студентов вузов. –М.: ЮНИТИ –ДАНА, 2005. – 127с.
25. Грайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем: підруч. - К.: Видавнича група BHV, 2009. - 608 с.
26. Гребенюк А.В. Искусство ведения информационной войны// Корпоративные системы.- 2006.- №2.- С.58-61.
27. Денісова О.О. Інформаційні системи і технології в юридичній діяльності: Навч. посіб.- К.: КНЕУ, 2004.- 315 с.
28. Задірака В.К. Методи захисту фінансової інформації/ В.К.Задірака, О.С.Олексюк.- Тернопіль: Збруч, 2000.- 460 с.
29. Игнатьев Д. Настольная энциклопедия Public Relations/ Д.Игнатьев, А.Бекетов, Ф.Сарокваша.- М.: Альпина Паблишер, 2002.- 229 с.
30. Информация: поиск, анализ, защита/ Авт-сост. Кузнецов И.Н.- Мн.: Амалфея, 2002.- 320 с.
31. Казинов И.Д. Контроль за несанкционированной утечкой информации// Корпоративные системы.- 2006.- №2.- С.54-55.
32. Карпенко С.Г., Іванов Є.О. Основи інформаційних систем і технологій: Навч. посіб. - К.: МАУП, 2007. - 264 с.
33. Костров А.В. Основы информационного менеджмента: Учеб. пособ.- М.: Финансы и статистика, 2003.- 336 с.
34. Лейхифф Дж. М., Пенроуз Дж. М. Бизнес – коммуникации. – Спб.: Питер, 2001 – 246 с.
35. Ліпкан В.А. Інформаційна безпека Україна в умовах євроінтеграції: Навч. посіб./ В.А.Ліпкан, Ю.Є.Максименко, В.М.Желіховський.- К.: КНТ, 2006.- 280 с.
36. Лодон Д. Управление информационными системами/ Д.Лодон, К.Лодон; Пер. с англ. Трутнев Д.Р - 7-е изд.- Спб.: Питер, 2005.- 912 с.
37. Макаренко Є.А. Європейська інформаційна політика: Монографія.- К.: Наша культура і наука, 2000.- 368 с.
38. Матвієнко О.В. Основи менеджменту інформаційних систем: Навч. посіб./ О.В.Матвієнко, М.Н. Цивін.- 2-ге вид., перероб. та доп.- К.: ЦУЛ, 2005.- 176 с.
39. Мейтленд Я. Рабочая книга PR-менеджера.- Спб.: Питер, 2007.- 176 с Мельников Ю. Нападения на информационные системы банка из Интернета/ Ю.Мельников, А.Теренин// Финансовые рынки и ценные бумаги.- 2003.- №14.- С.19-23.
40. Морзе Н. В. Основи інформаційно-комунікаційних технологій. - К.: Видавнича група BHV, 2006. - 352 с.
41. Мойсеєв В.А. Паблік рілейшнз: Навч. посіб.- К.: Академвидав, 2007.- 224 с.
42. Новий російсько-український словник з інформатики: Основні терміни. Близько 3300 термінів. / Уклад. Н. Я. Гінзбург, Л.І. Белоусова та ін. – Х.: «Корвін», 2002. - 656 с.
43. Осовська Г.В. Комунікації в менеджменті: Курс лекцій. – К.: Кондор, 2006. – 664 с.
44. Почепцов Г.Г. Коммуникативные технологии двадцатого века.- М.;К.: Рефл-бук;Ваклер, 2002.- 352 с.
45. Симионов Ю.Ф. Информационный менеджмент/ Ю.Ф.Симионов, В.В.Бормотов.- Ростов н/Д: Феникс, 2006.- 250 с.
46. Соколов А.В. Защита от компьютерного терроризма: Справочн. пособие/ А.В.Соколов, О.М.Степанюк.- Спб.: БХВ-Петербург: Арлит, 2002.- 496 с.
47. Сорока П.М., Сорока Б.П. Інформаційний менеджмент: навч. посіб./ за наук. ред. О.Д. Гудзинського. - К.: Ун-т "Україна", 2008. - 535 с.
48. Сурмин Ю.П. Теория социальных технологий: Учеб. пособие/ Ю.П.Сурмин, Н.В.Туленков.- К.: МАУП, 2004.- 608 с.

49. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій: Навч. посіб./ Петрик В.М., Штоквиш О.А., Полевий В.І. та ін.- К.: Росава, 2006.- 208 с.
50. Теория и практика связей с общественностью/ Кочеткова А.В., Филлипов В.Н., Скворцов В.Н., Тарасов А.С.- Спб.: Питер, 2006.- 240 с.
51. Уотсон Т. Методы оценки деятельности PR - подразделения компании: Лучшее практическое руководство по планированию, исследованиям и оценке связей с общественностью = Evaluating public relations: A best guide to public relations planning, research and evaluation/ Т.Уотсон, П.Нобл; Пер.с англ.- Днепопетровск: Баланс Бизнес Букс, 2006.- 272 с.
52. Харченко Л.С. Інформаційна безпека України: Глосарій/ Л.С.Харченко, В.А.Ліпкан, О.В.Логінов; Ред. Р.А.Калюжний.- К.: Текст, 2004.- 136 с Цыганов В. Медиа-терроризм. Терроризм и средства массовой информации.- К.: Ника-центр, 2004.- 120 с.
53. Щедрин А.Н. Электронные информационные ресурсы в информационной экономике.- Донецк, 2003.- 232 с.
54. Юдін О.К. Інформаційна безпека держави: Навч. посіб./ О.К.Юдін, В.М.Богуш.- Х.: Консум, 2005.- 576 с.
55. Доступ до інформації та електронне урядування/ Авт.-упорядники Демкова М.В., Фігель М.В. - К.: Факт, 2004. - 336 с
56. Інформаційні системи в менеджменті: підруч./ [Новак В. О., Симоненко Ю. Г., Бондар В. П. та ін.]. - К.: Каравела, 2008. - 616 с.
57. Інформаційні технології. Нормативна база/ Пашутинський Є. К. - К.: КНТ, 2005. - 500 с