Коцюк Ю.А.

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА СФЕРА ТА ЇЇ ПСИХОЛОГІЧНИЙ ВИМІР У ДІЯЛЬНОСТІ МЕНЕДЖЕРА

У статті розглядаються інформаційно-комунікаційні аспекти діяльності менеджера в умовах активного розвитку та використання комп'ютерних інформаційних технологій. Основна увага фокусується на інформаційній безпеці особистості менеджера.

The article takes the view of informational and communicative aspects of manager's activity in the conditions of active development and usage of computer informational technologies. The main attention is focused on the informational security of the personality of manager.

Важливість спеціальності менеджера не підлягає жодним сумнівам у соціальному, економічному та політичному житті сучасної України, так як ця професія є «найбільш складною, універсальною та відповідальною серед існуючих» [, 215]. Процес структуризації організацій спричинив появу великої кількості посад «керівників підрозділів», яких справедливо (правда поки що неофіційно) називають офіс-менеджерами, що в свою чергу каже про її поширеність. Тому й не дивно, що вимоги, що ставлять до знань, вмінь, навичок та індивідуальних здібностей особистості менеджера, постійно зростають. Разом з тим знання про закономірності управління, про психологічні особливості поведінки людини в організації розглядаються сьогодні, по суті, як невід'ємний компонент загальної культури особистості спеціаліста будь-якого профілю. «Де б не працював майбутній спеціаліст та чим би він не займався, він завжди інтегрується у «світ організацій», в систему управління, займаючи в ній певне місце (нерідко – керівне)» [, 5].

Якщо виходити з розуміння менеджменту як загальної і головної функції суспільства [, 37], цілком слушним, зокрема, виглядає звернення до проблематики значимості інформаційно-комунікаційної сфери у роботі менеджерів. На фоні інтенсивного розвитку інформаційних технологій особливої актуальності набувають питання інформаційної та інформаційно-психологічної безпеки, які неодноразово розглядалися у наукових доробках Б. Анина, В. Голубєва, М. Іванова, Г. Грачова, Г. Ложкіна, О. Столяренко, С. Назаренко, А. Мануйло, А. Петренко, Е. Андрєєва, А. Миронова, С. Рощіна [; ; ; ; ; ; ; ; ;]. Проте, не зважаючи на велику кількість публікацій, легко помітити певну розмежованість, що спостерігається у працях присвячених інформаційній безпеці, та, власне, працям, пов’язаним з інформаційно-психологічною безпекою.

Дана стаття ставить за мету дослідити роль інформаційно-комунікаційної сфери у діяльності менеджерів, акцентуючи увагу на зв’язку інформаційної безпеки особистості із станами психологічного комфорту.

Інформаційно-комунікаційна сфера суспільства пронизує всі інші сфери суспільства (економічну, соціальну, політичну, гуманітарну) і виконує функції, подібні кров'яній системі людини, яка забезпечує життєдіяльність усього організму.

З усіх сфер суспільства (правової, економічної, соціальної, політичної, гуманітарної та ін.) інформаційно-комунікаційна сфера розвивається найдинамічніше. Бурхливий розвиток Інтернету, мультимедіа, мобільного зв'язку тощо виступив потужним каталізатором модернізації насамперед економічної сфери суспільства. Нині вже нікого не здивуєш такими поняттями, як електронний бізнес (e-business), електронна комерція (e-commerce) тощо. А економіка, як головний рушійний генератор глобалізаційних процесів, зумовила кардинальні зміни у правовій, політичній, соціальній, гуманітарній та інших сферах суспільства.

Комунікація та інформація мають надзвичайно важливе значення в житті суспільства. Особливої ваги вони набувають у суспільстві, що стоїть на

шляху глобалізації. Останнє характеризується революційним розвитком інформаційно-комунікаційних технологій, які використовуються на всіх рівнях, у всіх областях, галузях, територіальних і часових просторах управління. За таких умов інформаційно-комунікаційна сфера заслуговує особливо уважного розгляду, проте, для глибшого розуміння самого поняття «комунікація» слід також розглянути й поняття «спілкування».

Спілкування є однією з універсальних реальностей буття людини, специфічним видом і необхідною умовою її діяльності. Від нього значною мірою залежить психологічний клімат в організації, на підприємстві, їх організаційна і виробнича мобільність, конкурентні позиції на ринку. Його характер обумовлюється етнічним, професійними, віковим, тендерними та багатьма іншими параметрами, які необхідно знати і враховувати, адже правильно організоване спілкування не тільки забезпечує ефективний обмін інформацією, а й дає змогу глибше пізнати партнера, спрогнозувати особливості подальшої ділової взаємодії з ним, іноді розпізнати за начебто вишуканими манерами некоректні наміри, тощо. А багато управлінських проблем є породженням саме непрофесійного, невмілого спілкування.

Спілкування – сукупність зв’язків і взаємодій індивідів, груп, спільнот, під час яких відбувається обмін інформацією, досвідом, уміннями, навичками і результатами діяльності [, 8]. При спілкуванні завжди відбувається обмін інформацією – комунікація. Однак комунікація і спілкування не тотожні за своїм змістом.

Комунікація (лат. communico – спілкуюсь із кимось) – смисловий та індивідуально-змістовний аспект соціальної взаємодії; обмін інформацією у різноманітних процесах соціальної взаємодії.

Зіставлення обох понять дає підстави для висновків, що «спілкування» є загальним за своїм змістом, а «комунікація» – конкретним, яке позначає лише один із його типів (соціальну взаємодію).

Комунікативний процес – обмін інформацією між індивідами або їх групами, метою якого є точне й повне засвоєння повідомлень, що містять певну інформацію[, 15]. У цьому процесі взаємодіють такі базові елементи:

- відправник – особа, яка генерує ідеї, або збирає і передає інформацію:
- повідомлення – закодована за допомогою символів інформація;
- канал (засіб) передавання інформації;
- одержувач – особа, якій призначена інформація і яка її інтерпретує.

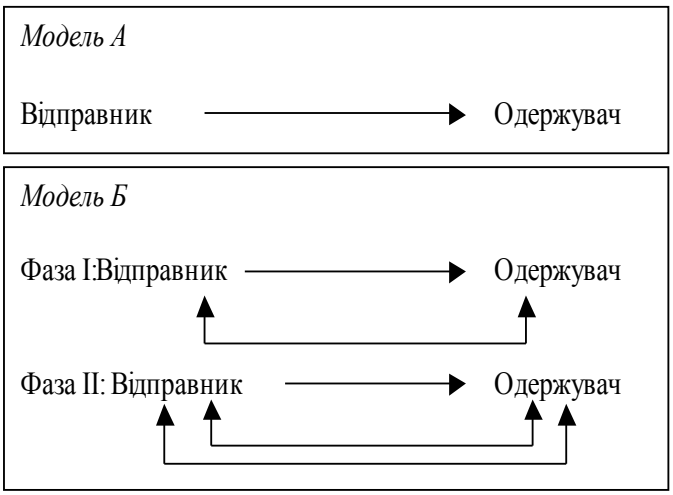

Рис. 1 Базові моделі передавання інформації

Одним із етапів комунікативного процесу є передавання інформації. На цьому етапі відправник використовує канал (засіб) передавання інформації для доставки повідомлення одержувачу. Йдеться власне про фізичне переміщення повідомлення від відправника до одержувача.

Існує дві базові моделі передавання інформації: без зворотного зв'язку і зі зворотнім зв'язком (модель А і модель Б) (див. Рис. 1.7) [, 17].

Модель А не передбачає зворотного зв'язку, тобто відправник не знає, як відреагував на інформацію одержувач. Модель Б передбачає ефективний зворотній зв'язок під час комунікації.

Обмін інформацією є ефективним, якщо одержувач не спотворено зрозумів ідею і виконав очікувані відправником дії, тобто, відправивши повідомлення відповідь, здійснивши зворотній зв'язок.

Отож управління будь-яким об'єктом (галуззю, підприємством, підрозділом тощо) – це процес, який неможливий без отримання, опрацювання і передачі інформації. Інформація об'єднує працівників один з одним і з організацією в цілому. Іншими словами, саме інформація дозволяє робітникам розумової праці виконувати свою роботу [, 170].

Під інформацією розуміють відомості про навколишній світ і про процеси, які відбуваються в ньому, та їх сприйняття людиною або спеціальними приладами. З точки зору змісту або сфери діяльності, у якій використовується інформація, її умовно поділяють на управлінську, наукову, технічну, медичну тощо.

Управлінська інформація – це інформація, якою послуговуються заклади, організації, підприємства з метою управління відповідними об'єктами []. Управлінська інформація повинна бути повною, оперативною, достовірною. Повноту інформації характеризує її обсяг, який має бути необхідним і достатнім для прийняття управлінських рішень. Брак інформації призводить до прийняття хибних рішень або знижує їх обґрунтованість; надлишок інформації, наслідком якого є збільшення обсягу повідомлення без підвищення його інформативності, пов'язаний з додатковими витратами праці і часу робітників-управлінців. Інформація повинна бути оперативною, тобто такою, щоб за час її передачі й опрацювання стан об'єкта, до якого вона відноситься, не змінився. Достовірність інформації визначається ступенем відповідності її змісту об'єктивного стану речей та явищ. Зростання масштабів виробництва, науково-технічний прогрес, збільшення кількості господарчих одиниць і зв'язків між ними, вироблених товарів та швидкість змін економічної, технічної і соціальної ситуації приводять до зростання обсягів інформації, необхідної для ефективного управління об'єктами промисловості.

Більшість інформації, яка використовується в управлінні, фіксується. Це обов’язковий елемент управлінської діяльності, оскільки в сучасних умовах отримувати, зберігати і передавати інформацію можливо тільки за попередньої її фіксації []. Цінність інформації – це найважливіший критерій при прийнятті будь-якого рішення про її захист. Відомий наступний поділ інформації по рівню важливості []:

- життєво важлива незамінна інформація, наявність якої необхідна для функціонування комп'ютерної системи, організації і т.п.
- важлива інформація – інформація, яка може бути замінена чи відтворена, але процес відтворення якої дуже складний чи пов'язаний із значними затратами;
- корисна інформація – інформація, яку важко відновити, однак комп'ютерна система чи організація можу успішно функціонувати і без неї;
- несуттєва інформація.

Цінність інформації зазвичай міняється з часом і залежить від ступеня відношення до неї різних груп користувачів, що беруть участь у процесі обробки інформації [].

Існує також поділ інформації по рівню таємності, конфіденційності. До таємної інформації належить інформація, що містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі []. Ознаками таємної інформації є наявність [, 7], по-перше, законних користувачів, по-друге, незаконних користувачів (порушників, противників, конкурентів), які стараються оволодіти цією інформацією, для того, щоб використати її собі на користь, а законним користувачам на шкоду.

Конфіденційна інформація - це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених ними умов [].

Мета створення систем безпеки – попередження наслідків навмисних і випадкових деструктивних впливів, наслідком яких можуть бути знищення, модифікація чи відплив інформації, а також дезінформація. У випадку, якщо об'єкт атаки супротивника – якийсь із компонентів системи (апаратні засоби чи ПЗ), то можна говорити про переривання, коли компонент системи стає недоступним, втрачає працездатність чи просто втрачається в результаті крадіжки; про перехват та/чи модифікацію, коли супротивник отримує доступ до компонента і/чи можливість маніпулювати ним; про підробку, коли супротивнику вдається додати у систему деякий компонент чи процес (програмне забезпечення, що здійснює руйнування), файли чи записи в них [;]. Ефективна система безпеки повинна забезпечити [; ; ;]:

- таємність усієї інформації чи найбільш важливої її частини;
- достовірність (повноту, точність, адекватність, цілісність, автентичність) інформації, працездатність системи у будь-який момент часу;
- своєчасний доступ користувачів до необхідної їм інформації та ресурсів системи;
- захист авторських прав, прав власників інформації, можливість вирішення конфліктів;
- розмежування відповідальності за порушення встановлених правил інформаційних відносин;
- оперативний контроль за процесами управління, обробки та обміну інформацією, так звані засоби контролю безпеки (сторожеві процеси, системи сканування, моніторингу, засоби виявлення і реєстрації аномальних дій користувачів чи поведінки компонентів АСОД[1]).

Варто зауважити при цьому два важливих факти. По-перше, в залежності від об'єкта захисту можливе встановлення різних пріоритетів серед перерахованих властивостей системи безпеки. У випадку захисту державних установ найвищий пріоритет має таємність інформації. При

[1] АСОД – Автоматизовані системи обробки даних

захисті, на приклад, банківської платіжної системи найбільш важливою властивістю варто визнати забезпечення своєчасного доступу користувачів до необхідних їм ресурсам системи та достовірність інформації. По-друге, існує протиріччя, яке важко вирішити, між ефективним виконанням системою своїх основних функцій і ступенем забезпечення у ній необхідного рівня безпеки. Чим вищі вимоги висуваються до безпеки системи, тим більша кількість її ресурсів виявляється задіяною для забезпечення цих вимог, відповідно, тим дискомфортніше користувачам, що працюють у цій системі. І навпаки, чим більше ресурсів виділяється користувачам, тим менше їх лишається для вирішення задачі забезпечення безпеки.

Причинами випадкових деструктивних впливів, яких інформація зазнає в процесі вводу, зберігання, оброки, виводу та передачі, можуть бути []:

- відмова та збої обладнання;
- перешкоди на лініях зв'язку під впливом зовнішнього середовища;
- помилки людини, як ланки системи;
- помилки розробників апаратного та/чи програмного забезпечення;
- аварійні ситуації;

До методів захисту від випадкових впливів можна віднести:

- стійке до перешкод кодування;
- придатне для контролю, стійке до відмов обладнання;
- процедури контролю справності, працездатності і правильності функціонування обладнання;
- самоконтроль чи само тестування;
- контроль виконання програм та мікропрограм.

Навмисні загрози пов'язані з діями порушника, який при цьому може скористатися як штатними (законними), так і іншими каналами доступу до інформації в АСОД. При цьому, згідно праць великого числа дослідників та науковців (див. [; ; ; ;]) в результаті дій порушника, який може бути як

незаконним так і законним користувачем, інформація піддається таким загрозам, як:

- крадіжка носіїв інформації чи обладнання;
- виведення компонентів системи із ладу чи організація неправильного функціонування;
- приведення системи у стан, який вимагає незапланованих затрат ресурсів (наприклад, на обслуговування поступаючих повідомлень та запитів, на ведення оперативного контролю, на відновлення працездатності, на усунення спроб порушення безпеки і т.д.);
- несанкціоноване копіювання програм і даних;
- несанкціонований доступ до таємної інформації (такої, що зберігається чи передається каналами зв'язку);
- знищення чи несанкціонована модифікація інформації чи програмного забезпечення;
- фальсифікація повідомлень (наприклад видача себе за іншого користувача; санкціонування недозволеного обміну інформацією; нав'язування раніше пересланого повідомлення; приписування авторства повідомлення, сформованого самим порушником, іншій особі і т.п.);
- відмова від факту отримання чи відправлення повідомлення (так зване ренегатство);
- відмова від факту отримання чи відправлення повідомлення у певний момент часу;
- порушення протоколу обміну інформацією з метою його дискредитації;
- імітація роботи системи, аналіз поведінки компонента, який зацікавив, чи аналіз трафіка з метою отримання інформації про ідентифікатор користувача, пошуку каналів витоку інформації, каналів прихованого впливу на об'єкт, про правила вступу у зв'язок і т.д.;

- вхід у системи під виглядом законного користувача (наприклад, використовуючи паузи у діях останнього, ідентифікатори, які стали відомі в результаті аналізу чи іншим шляхом);
- розрив зв'язку і подальша робота з системою під виглядом законного користувача;
- створення перешкод процедурі обміну повідомленнями між користувачами системи.

Для кожного типу загроз зазвичай можна запропонувати один чи декілька заходів протидії, метою застосування яких є зменшення ризику чи то за рахунок зменшення вірогідності здійснення загрози, чи то за рахунок зменшення наслідків реалізації загрози. У сукупності такі заходи створюють політику безпеки. Основними характеристиками кожного заходу протидії є ефективність і вартість, саме вони є основою для проведення раціональної з економічної точки зору політики безпеки. При оцінюванні загроз зі сторони супротивника варто врахувати також вартість їх реалізації. "Нормальний" супротивник не буде витрачати на реалізацію загрози більше заходів, ніж він може отримати від наслідків її виконання. Тому однією із цілей заходів протидії може бути збільшення ціни порушення безпеки системи до рівня, який перевищує оцінку очікуваного супротивником виграшу. Ефективним заходом захисту може бути всього на всього оперативне виявлення факту реалізації загрози, враховуючи різноманітні економічні та соціальні санкції, які чекають на порушника у випадку виявлення його дій.

Виділяють наступні методи захисту інформації від навмисних деструктивних дій (Див. [; ; ;]):

- методи забезпечення фізичної безпеки компонентів системи;
- обмеження доступу;
- розмежування доступу;
- поділ доступу (привілеїв) – отримання доступу лише при одночасному пред'явленні повноважень усіх членів групи;

- криптографічне перетворення інформації та реалізовані на його основі криптографічні протоколи;
- контроль та аудит доступу;
- законодавчі засоби;
- принципи та правила роботи в системі, що зменшують ризик порушення безпеки, наприклад регулярне створення резервних копій системи чи найбільш важливих її компонентів, встановлення певної процедури копіювання;
- формування етичних норм для користувачів, так званого "кодексу поведінки", згідно якого вважаються неетичними будь-які навмисні дії, які можуть порушити роботу системи.

До психологічних та соціально-психологічних факторів, що впливають на формування інформаційно-комунікаційної мережі відносять []:

- інтелект робітника – рівень його розвитку повинен відповідати посаді що даний робітник займає;
- комунікативні якості робітника – комунікабельність, відкритість, спостережливість, здатність легко сприймати інформацію та швидко і без спотворень передавати її;
- комунікаційний стиль робітника – зокрема виділяють наступні стилі: "відкриття себе", "реалізація себе", "замкнутися в собі", "захист себе", "утримати себе";
- інформаційні навантаження – здатність конкретного робітника сприймати певний об'єм інформації за одиницю часу;
- психологічна інтеграція робітника в інформаційну мережу – передбачає розуміння робітником своєї ролі в інформаційно-комунікаційній мережі, усвідомленням власної відповідальності;
- пізнавальні та семантичні бар'єри – виникають між суб'єктами мережі, які мають різний рівень розуміння інформації, що передається і використовують різну термінологію;

- взаємовідносини робітників – міжособистісні, особистісно-групові, міжгрупові, а також загальна психологічна атмосфера в колективі та на підприємстві;
- психологічні властивості вертикальних, горизонтальних та діагональних комунікацій – так існують дані, що найкраще інформація поширюється горизонтальними каналами, і досягає ефективності 90% в той час як у напрямку знизу вверх доходить лише 10% відсотків інформації а у зворотному – 20-25%;
- особливості відношення топ-менеджера до інформації, що поступає – в багатьох випадках, інформація, що поступає до керівника від підлеглих, залежить від особистості керівника, так при жорсткій реакції на негативні новини, підлеглі починають приховувати негативну інформацію;
- залежність психологічної складності передачі повідомлень від їх форми та засобів, що використовуються для передачі – так передача повідомлень в усній формі більш схильна до спотворення на відміну від паперової чи електронної форми, крім того значний вплив на спотворення повідомлення відіграє кількість посередників, через які проходить повідомлення, чим їх менше, тим краще;
- психологічні складності багатоступінчатих та багатоланкових комунікацій – за звичай чим складніша загальна схема комунікації тим більше змінюється повідомлення при передачі;
- психологічні складності, викликані формальною організацією – так централізована схема передбачає зростання внутрішніх комунікацій, проте призводить до спотворення та втрат інформації, в той час як децентралізована схема характеризується зростанням зовнішніх комунікацій та надмірністю повідомлень;
- зовнішні соціально-психологічні впливи – до них відносять складності в отриманні інформації, навмисними труднощами, що створюються

конкурентами, підкиданням дезінформації, перехопленням повідомлень, дешифруванням конфіденційної інформації тощо.

Таким чином для забезпечення в організації ефективної комунікативної мережі менеджеру слід враховувати цілу низку різноманітних факторів, більшість яких залежить безпосередньо від нього, від його знань, вмінь, навичок, від його психологічного настрою врешті решт, чим комфортніше почуватиметься менеджер, тим більше шансів у нього досягнути успіху у процесі організації Разом з тим аналіз загроз безпеки в АСОД, тенденції розвитку інформаційних технологій дають усі підстави стверджувати про постійне зростання ролі криптографічних методів при вирішення задач автентифікації в інформаційних системах, забезпечення таємності даних при їх передачі через відкриті канали зв'язку, забезпечення юридичної значимості результатів інформаційного обміну.

Аналізуючи усе вище сказане, приходимо до висновку, що у комплексі знань, вмінь та навичок сучасного менеджера обов’язково повинні бути такі, що пов’язані із криптографічними методами захисту інформації. Вивчення криптографії дозволить знизити рівень дискомфорту робітника, що виникає при використанні інформаційних систем із використанням високого ступеню захисту, підвищити стан його психологічної готовності до навмисних чи ненавмисних деструктивних дій у інформаційно-комунікацій сфері.

Література:

1. Андреев Э.М., Миронов А.В. Социальные проблемы интеллектуальной уязвимости и информационной безопасности /Э.М.Андреев, А.В.Миронов // Социально-гуманитарные знания. – 2000. - №4. – С.169-179.
2. Анин Б.Ю. Защита компьютерной информации. СПб.:БХВ – Санкт–Петербург, 2000. – 384 с.
3. Анин Б.Ю. Защита компьютерной информации. СПб.:БХВ – Санкт–Петербург, 2000. – 384 с.

4. Анохин М.И., Варновский Н.П., Сидельников В.М., Ященко В.В. Криптографія в банковском деле. М.: МИФИ, 1997. – 247 с – http://www.cryptography.ru/db/msg.html?mid=1169307

5. Баричев С.У. Гончаров В.В. Серов Р.Е. Основы современной криптографии. - М.: Горячая линия – Телеком", 2001.

6. Бурега В.В, Любчук О.К. Економічна психологія в схемах і таблицях: Навч.-метод. посібник / Донецька держ. академія управління. – Донецьк : ДонДАУ, 2003. – 63с.

7. Введение в крипторгафию / Под. общ. ред. В.В. Ященко. М.:МЦНМО: ЧеРо, 1998. – http://www.cryptography.ru/db/msg.html?mid=1161235

8. Введение в крипторгафию / Под. общ. ред. В.В. Ященко. М.:МЦНМО: ЧеРо, 1998. – http://www.cryptography.ru/db/msg.html?mid=1161235

9. Верховна Рада України; Закон від 02.10.1992 № 2657-XII, ЗАКОН УКРАЇНИ Про інформацію, Відомості Верховної Ради (ВВР), 1992, N 48, ст. 650.

10.Голубєв В. Теоретико-правові питання захисту інформації в автоматизованих системах // Центр дослідження комп'ютерної злочинності – http://crime-research.iatp.org.ua/library/Golubev_new_ukr.doc

11.Грачев Г.В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты – М.: Изд-во РАГС, 1998. – 125 с.

12.Доценко В.И., Фараджев Р.Г., Чхартишвили Г.С. Свойства последовательностей максимальной длины с *P*–уровнями // Автоматика и телемеханика. 1971. №8 С. 189-194.

13.Друкер Питер Ф. Задачи менеджмента в XXI веке .– М.: Вильямс, 2004. – 272 с.

14.Друкер Питер Ф. Практика менеджмента: Пер. с англ.: – М.: Издательский дом "Вильямс", 2002. – 398.
15.Зубенко Л.Г., Нємцов В.Д., Чупріна М.О. Ділові папери в менеджменті: Навчальний посібник .– Київ: ТОВ "УВПК "ЕксОб", 2003.– 272 с.
16.Зубенко Л.Г., Нємцов В.Д., Чупріна М.О. Ділові папери в менеджменті: Навчальний посібник .– Київ: ТОВ "УВПК "ЕксОб", 2003.– 272 с.
17.Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. М.: КУДИЦ-ОБРАЗ, 2001 – 368 с.
18.Информационно-психологическая безопасность избирательных кампаний /Под редакцией Брушлинского А.В. и Лепского В.Е. М.: Институт психологии РАН, 1999. – 98 с.
19.Карпов А. Психология менеджмента. Учебное пособие, – М.: «Гардарики» 2005. – 584 с. – http://www.bizbook.ru/index.php?rubrik_id=28001&book_id=17398
20.Ложки Г.В. Информационно-психологическая безопасность личности // Персонал. – 2002. – № 3. – С. 78–81.
21.Мануйло А.В., Петренко А.И. Информационно-психологическая безопасность системы социально-политических отношений современного общества //
22.Мельников В.В. Защита информации в компьютерных системах. М.: Финансы и статистика: Электроинформ, 1997. – 368 с.
23.Моисеенков И. Основы безопасности коп'ютерных систем // КомпютерПресс. 1991. № 10. С. 19–24. 1991. № 11. С. 7–21.
24.Психологія праці та професійної підготовки особистості: Навчальний посібник / За ред. П.С. Перепелиці, В.В. Рибалки. – Хмельницький: ТУП, 2001. – 330с.
25.Рощин С.К. Некоторые вопросы информационно-психологической безопасности российского общества // Проблемы информационно-психологической безопасности. – М.: ИП РАН, 1996. – С. 27–32.

26.Столяренко А.М., Амаглобели Н.Д. Психология менеджмента: Учеб. пособие. – М.: ЮНИТИ-ДАНА, 2005. – 608 с.
27.Хміль Ф.І. Ділове спілкування: навчальний посібник для студентів вищих навчальних закладів. – К.: “Академвидав”, 2004. – 280 с.