захисту."Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 8, 2004. С. 39-43. ***6.*** *Кононович В. Г., Тардаскіна Т. М. Алгоритм розподілу ресурсів інформаційної безпеки документальних телекомунікацій. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 9, 2004. С 152-161.* ***7.*** *Носов В., Манжай А. Метод проектирования оптимальной системы защиты информации. "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 8, 2004. С. 94-103.* ***8.*** *ITU-T Recommendation X.805. Security architecture for system providing end-to-end communications. С. 28.* ***9.*** *Ліцензійні умови провадження діяльності у сфері телекомунікацій з надання послуг фіксованого міжнародного міжміського, місцевого зв'язку з правом технічного обслуговування та експлуатації телекомунікаційних мереж і надання в користування каналів електрозв'язку" (наказ Держкомзв'язку № 132 від 17. 06. 2004 р.), С. 25.* ***10.*** *Ліцензійні умови провадження діяльності у сфері телекомунікацій з технічного обслуговування і експлуатації мереж ефірного теле- та радіомовлення та телемереж, надання в користування каналів електрозв'язку" (наказ Міністерства транспорту та зв'язку України № 984 від 10. 11. 2004 р.) С. 20.* ***11.*** *Тесля В. Я., Бабосюк А. Л., Сикорский В. В., Рудниченко А. Е. Концептуальные подходы к технологии сетей нового поколения NGN // "Зв'язок", № 2, 2004. С.70-73.* ***12.*** *ITU-T Recommendation X.200. Reference model of open systems interconnection for CCITT applications. Geneva. 1991. С. 75; (Стандарт ISO 7498-1:1984. Базова модель ВВС).* ***13.*** *ITU-T Recommendation X.800. Security architecture for Open Systems Interconnection for CCITT applications. Geneva.1991. С. 48; (Стандарт ISO 7498-2:1989. Архітектура безпеки ВВС).*

УДК 621.395:338.47

ОРГАНІЗАЦІЙНО-УПРАВЛІНСЬКІ АСПЕКТИ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Тетяна Тардаскіна

Одеська національна академія зв'язку ім. А. С. Попова

Анотація: **Розроблено організаційні рекомендації управління персоналом системи інформаційної безпеки.**

Summary: **Development organizational recommendation personal management of information security system.**

Ключові слова: **Інформація, інформаційна безпека, управління персоналом, кадровий консалтінг.**

Вступ

Проблема захисту мереж телекомунікацій та інформації, що циркулює в них, вимагає великої уваги в зв'язку з тим, що в інформаційному суспільстві, до якого прагне Україна, захист інформаційного середовища стає таким же важливим для кожного громадянина, суспільства і держави, як і захист навколишнього середовища, власного майна.

В Україні до інформаційних ресурсів прийнято відносити технічну інфраструктуру й інформацію, що в ній обробляється, циркулює і зберігається. Недостатня увага приділяється колосальному пласту питань, який впливає на забезпечення безпеки інформаційних систем: діяльність персоналу, адміністративна і юридична підтримка. Проблема захисту ускладнюється тим, що загрози, від яких доводитися захищати мережі та інформацію, дуже різноманітні і мають навіть різне походження: природне, техногенне, антропогенне. Однак для загроз природного, техногенного та ненавмисного антропогенного походження прогноз частково можливий, а наслідки рідко корелюються із діями або інформацією користувачів, тому рідко бувають катастрофічними. Принципи захисту від таких загроз відомі, і, як правило, їх можна реалізувати під час розробки, впровадження та експлуатації мереж телекомунікацій [1]. Ця проблема вирішувалась у багатьох суміжних областях безпеки, управління та прийняття рішень [2 – 7], але відносно управління персоналом системи інформаційної безпеки така задача остаточно не вирішена.

Слід відзначити, що багато питань інформаційної безпеки вже вирішуються системою технічної експлуатації, системою управління електрозв'язком, системою управління якістю та менеджменту телекомунікацій. Але це стосується в основному протидії техногенним загрозам інформаційним ресурсам. Антропогенні загрози враховуються мало. Водночас, необхідність управління персоналом тісно пов'язана з захистом комерційної таємниці фірми, бо персонал є одним з основних носіїв інформації, і як вважають фахівці, імовірність витоку інформації через підкуп, переманювання співробітників складає 43%, а через вивідування – 24%. Найнепередбачуваніші загрози виникають внаслідок навмисної, особливо зловмисної антропогенної діяльності, саме захист від таких загроз найбільш складний і потребує особливої уваги при

розгляді стратегії розвитку мереж телекомунікацій [1, 7].

Уразливість будь-якої системи, як правило, оцінюється найбільш слабкою ланкою. Накопичений досвід недвозначно показав, що найслабша ланка системи інформаційної безпеки підприємства – це власні співробітники. Необачність або просто необережність, неуважність одного співробітника може звести нанівець навіть найдійовіші контрзаходи технологічного характеру. Саме тому до міжнародних і національних стандартів з інформаційної безпеки включаються цілі розділи, присвячені роботі з персоналом підприємства [8].

З початку року в Україні було розкрито більш 40 тис економічних злочинів, які привели до втрат у розмірі близько 1 млрд. грн. Цифра вражає і змушує задуматися. Цілісність комерційної таємниці фірми на 80% залежить від правильного підбору, розміщення, грамотно поставленої роботи з кадрами, стабільності кадрового складу. Рішенню цієї проблеми і присвячена дана стаття.

Метою даної статті є розробка організаційних рекомендацій управління персоналом щодо становлення системи інформаційної безпеки.

У ринковій економіці виживання є важливою задачею будь-якого підприємства. Діяльність з управління персоналом є важливою гарантією того, що підприємство буде жити і процвітати. Адже саме люди обмежують або збільшують силу і слабкість підприємства. Людина з її потребами, мотиваціями і конкретними інтересами є наразі мірою прогресу і, коли фірма дійсно піклується про людей, це обов'язково відбивається на її діяльності.

І Основні віхи організаційних рекомендацій щодо управління персоналом системи інформаційної безпеки

Існує багато різних засобів несанкціонованого доступу до інформації. Але слід одразу ж відмітити, що ніякий окремо взятий засіб захисту не в змозі гарантувати адекватну безпеку. Надійний захист можливий лише за умови створення механізмів комплексного забезпечення безпеки. Виділяють три основні складові такого комплексу: нормативно-правові, технічні, організаційні засоби.

Нормативно-правові засоби захисту визначаються законодавчими актами держави, які регламентують правила використання, обробки та передачі інформації обмеженого доступу та встановлюють ступінь відповідальності за порушення цих правил. У ст. 34 Конституції України розглядається право громадян України на інформацію, забезпечення інформаційних процесів [9].

Уся сукупність технічних засобів поділяється на фізичні і апаратно-програмні та включає електричні, механічні, електромеханічні та електронні пристрої. Фізичні засоби реалізуються у вигляді автономних пристроїв та систем, що виконують функції загального захисту об'єктів, на яких обробляється інформація. Апаратні технічні засоби розміщують безпосередньо в обчислювальній техніці, в телекомунікаційній апаратурі чи в пристроях, що з’єднуються з подібною апаратурою за допомогою стандартного інтерфейсу. Програмні засоби представляють собою програмне забезпечення, що виконує функції захисту інформації.

Більш детально зупинимося на організаційних засобах. Людина не тільки є вмістилищем інформації, вона обробляє, аналізує її, та робить необхідні висновки і діє відповідно до них. Інформацію, що їй відома, вона може легко відтворювати, копіювати і поширювати, а також одержавши лише частину інформації стати власником значно більшого її обсягу [10]. Співробітники підприємства можуть виступати як об'єктом так і суб'єктом загроз, спрямованих на порушення економічної стабільності підприємства. Організаційні заходи захисту мереж та інформації передбачають охорону мережі телекомунікацій, особливо її системи управління, ретельний підбір та контроль діяльності персоналу, причетного до створення, впровадження й експлуатації мережі, встановлення режиму обмеженого доступу до окремих видів інформації, ретельну розробку комплектів інструкцій з технічного обслуговування і захисту мережного обладнання та інформації, регулярне інформування фахівців і керівників про чинне законодавство в сфері безпеки телекомунікацій та інформатики, застосування дисциплінарної, адміністративної та кримінальної відповідальності при виявленні порушення безпеки мереж телекомунікацій [1].

Основні віхи організаційних рекомендацій управління персоналом щодо становлення системи інформаційної безпеки на підприємстві можуть бути сформовані в такому вигляді.

1. На підприємстві має існувати детальна адміністративна політика відносна персоналу. Ця політика має детально регламентувати і мінімізувати права доступу співробітників до інформації, метою політики доступу є вимоги до регламенту використання доступної інформації.

2. Адміністративна політика має підкріплюватися не менш детальним моніторингом дій користувачів. Таким моніторингом мають бути охоплені всі без винятку користувачі, хто має легальні права доступу до інформації, налагодження апаратури, бази даних, операційних систем.

3. Виявлена розбіжність адміністративної політики і моніторингу може означати наявність «конфлікту

інтересів» підприємства та її персоналу.

4. Необхідно дотримуватись принципу «прозорості»: персонал повинен пояснювати усі свої дії з інформацією, які виявлені системою моніторингу.

5. Повинен існувати перелік корпоративних морально-етичних вимог, який чітко регламентує правила поведінки співробітника, що дозволяє виявити „конфлікт інтересів" і дає можливість керівництву застосувати, у разі потреби, адміністративні міри впливу.

6. З персоналом повинна проводитися багатопланова робота, метою якої є вироблення у людей етики корпоративної поведінки та відносин до ресурсів підприємства.

II Концептуальній підхід до управління персоналом і забезпечення інформаційної безпеки підприємства

Інформаційна безпека підприємства прямо зв'язана з економічною поведінкою її персоналу. В основі економічної поведінки лежать ціннісні орієнтири людей (гроші, статус, роль, ідеали). На економічну поведінку впливають різні фактори: технічний рівень виробництва, організація, нормування, оплата та умови праці, задоволення від праці, морально-психологічний клімат у колективі, освітній і культурний рівень працівника, характер суспільно-політичної активності в суспільстві та робочій групі [11].

Особливості проблеми захисту телекомунікаційних мереж та інформації пред'являють певні специфічні вимоги до персоналу, насамперед, до процесу їх діяльності з інформаційної безпеки. При підборі кандидатів, яким треба буде працювати із секретною інформацією, необхідно враховувати їх ділові, професійні, моральні якості та психологічні особливості [12].

Сформулюємо організаційно-психологічні заходи забезпечення економічної безпеки підприємства.

1. Перевірка персоналу і регламент роботи з персоналом. Перевірка співробітників, прийнятих на постійну роботу, повинна проводитися під час подачі заяви про прийом на роботу і включати наступні етапи:

- наявність позитивних характеристик (рекомендацій), однієї, що характеризує ділової якості, а другої – особисті якості;
- перевірку повноти і точності резюме (автобіографії) претендента на вакансію;
- підтвердження заявленого рівня освіти і професійної кваліфікації;
- незалежну ідентифікацію особистості (паспорт або йому подібний документ).

У тих випадках, коли посадові обов'язки, як при первісному надходженні на роботу, так і в результаті просування по службі, передбачають доступ до засобів обробки інформації, особливо до засобів обробки інформації з обмеженим доступом, комерційної та такої, що належить державі – підприємство повинно також перевірити становище співробітника. Співробітники, що займають відповідальні посади, повинні проходити таку перевірку регулярно [8].

2. Варто заохочувати пильність на робочих місцях, і передбачати шляхи, за допомогою яких співробітники могли б повідомляти про підозрілу діяльність.

3. Формування у співробітників почуття відповідальності за виконувану роботу і самостійності як виконавця.

4. Співробітники мають знати, що всі їхні дії контролюються.

Умови наймання повинні визначати обов'язки і відповідальність співробітника за інформаційну безпеку. При необхідності, така відповідальність повинна зберігатися протягом визначеного часу після звільнення співробітника. Повинні бути також зазначені дії, що починаються в тому випадку, якщо співробітник нехтує вимогами до інформаційної безпеки [8].

5. Впровадження діючої системи матеріальної і моральної мотивації кожному члену колективу.

6. Забезпечення участі всього персоналу, звичайно за умови, коли це є можливим, у прийнятті принципових, стратегічних рішень.

7. Дотримання політики інформаційної безпеки в значній мірі є елементом корпоративної культури. Тому цими відносинами необхідно керувати.

8. Необхідне навчання і регулярна перепідготовка кадрів, як в напрямку основної діяльності, так і з питань інформаційних технологій, діловодства і безпеки.

Усі співробітники підприємства, а при необхідності, і сторонні користувачі, повинні пройти навчання за регламентом і процедурами, які використовуються на підприємстві і регулярно отримувати інформацію про зміни в них. Така програма підготовки стосується вимог до забезпечення безпеки, питань юридичної відповідальності і засобів керування діловими процесами, а також включає навчання з правильного використання засобів обробки інформації (наприклад, процедури входу в систему, використанню програмного забезпечення), – перш, ніж буде надано доступ до інформації та засобів її обробки [8].

9. Розміщення кадрів відповідно до здібностей, кваліфікації, освіти, вислуги років, стану здоров'я та

інших факторів, які впливають на кар'єру і на посаду персоналу.

Діяльність служби персоналу, так чи інакше пов'язану з забезпеченням інформаційної безпеки, можна поділити на чотири основних напрямки:

1. підбір надійних і висококваліфікованих працівників;
2. захист конфіденційної інформації і персональних даних співробітників;
3. захист інформації, що знаходиться в головах співробітників і має цінність для організації, в якій вони працюють;
4. процес звільнення.

Найчастіше пошук нових співробітників входить у коло обов'язків служби персоналу, хоча нерідко підбір здійснюється безпосередньо керівниками тих ділових підрозділів, де відкрилася вакансія. Професійні знання і навички претендента оцінюють кваліфіковані фахівці саме того підрозділу, у якому новачок буде працювати. На жаль, при цьому часто забувають переконатися в надійності людини.

Перевірка персоналу в кожному підприємстві проходить по-своєму. Великі фірми можуть собі дозволити послуги відповідних державних структур, у той час як невеликі підприємства покладаються на досвід й інтуїцію свого керівництва і служби персоналу. Ефективність перевірок поки що залишає бажати кращого.

Захист інформації, що знаходиться в головах співробітників – це важливий напрямок у діяльності служби персоналу. На жаль, керівники більшості наших підприємств не розуміють, що знання і навички співробітників є одним із ключових інформаційних ресурсів підприємства, причому, за відсутності якого інші ресурси можуть стати марними. Для підприємства тяжкі наслідки можуть спричинити перехід до конкурентів ключових співробітників, їх відсутність на робочих місцях через хворобу або з інших причин. Імовірність втрати знань, які зберігаються в головах співробітників, є серйозною загрозою інформаційної безпеки підприємства. Для зменшення рівня цієї загрози можна знижувати зацікавленість співробітників у зміні місця роботи, для чого необхідно:

- стежити за середніми рівнями заробітної плати на ринку праці, і не допускати помітного відставання рівня зарплати від середнього рівня;
- не забувати про моральне заохочення співробітників, про створення сприятливого клімату в колективі; уважне і людяне відношення до співробітників не вимагає великих витрат, але найчастіше дає набагато більший ефект, ніж матеріальне заохочення;
- розвивати корпоративну культуру, яка включає лояльність до свого підприємства;
- впроваджувати програми переміщення працівників всередині підприємства, бо талановиті працівники – це джерело їх конкурентної переваги;
- уникати ситуацій, коли співробітник стає незамінним, вчасно готувати кадровий резерв; якщо обстановка на підприємстві сприятлива і співробітники упевнені у своєму майбутньому, в подальшому просуванні, – тоді вони, як правило, охоче передають свій досвід молодшим колегам;
- детально і ретельно описувати ділові процеси й операції на всіх ділянках, оформляючи ці описи у вигляді внутрішніх нормативних документів – інструкцій з виконання операцій. Мета – забезпечити правильне виконання дій навіть персоналом, незнайомим з даною ділянкою роботи. Необхідно також прописати правила передачі повноважень і функцій відсутніх співробітників;
- надавати співробітникам тільки ту інформацію, яка їм необхідна для виконання службових обов'язків; по можливості уникати ситуацій, коли співробітник має доступ до всієї інформації з визначеного критично-важливого питання. Корисно відслідковувати, з якою особливо цінною інформацією співробітники були ознайомлені (так, як це робиться в секретному діловодстві).

Звільнення персоналу – важливий і трудомісткий процес у діяльності служби персоналу. Особливо, звільнення людини, що працює з конфіденційною інформацією, являє загрозу економічній безпеці підприємства. Насамперед, потрібно з'ясувати причину звільнення (за власним бажанням, або його викрито в промисловому шпигунстві, або перехід до конкурентів), спробувати визначити справжню причину його рішення, проаналізувати і вирішити, потрібно його утримувати чи звільнити. Процес звільнення повинен включати відповідні етапи: написання співробітником заяви з повним розкриттям причини його рішення; організація передачі справ; здача співробітником усіх документів, ключів, пропусків; проведення інструктажу робітника, який звільняється, про зобов'язання та відповідальність за збереження таємниці конфіденційної інформації; виявлення обсягів відомої йому конфіденційної інформації (при шпигунстві – зміна всіх ключів, паролів, шифрів на конфіденційну інформацію та посилення контролю); документальне оформлення звільнення; виявлення майбутнього місця роботи.

Плинність кадрів в організації - показник, що характеризує існуючу в організації кадрову політику. Якщо плинність вище 5 %, то варто не тільки подумати про закріплення співробітників, але і звернути особливу увагу на взаємозамінність співробітників. Залишання посади кращого співробітника завжди

викликає додаткову напругу, і багато чого залежить від того, як підприємство підготовлено до цієї ситуації. Якщо робота організована так, що в підрозділах працівники можуть підмінити один одного, якщо ведеться регулярне навчання персоналу і створюється кадровий резерв, тоді зміна або звільнення посади будь-якого співробітника (незалежно від причин) не приведе до важких наслідків.

Корисно визначити найбільш відповідальні ділові процеси на підприємстві і простежити за тим, щоб не було фахівців – "монополістів", без яких неможливо обійтись. На жаль, на невеликих підприємствах окрему ділянку роботи звичайно веде тільки одна людина, і є ризик втратити не тільки самого співробітника, його знання і навички (при звільненні, хворобі і т. д.), але і контроль над цією ділянкою діяльності, тому що ніхто не зможе продовжити цю роботу. Інша сторона проблеми полягає в тому, що в "монополістів" з'являється можливість шантажувати керівництво.

Також важливо організувати навчання молодих співробітників на робочих місцях своїми старшими колегами, що можливо тільки за наявності мотивації в досвідчених працівників, коли "вчителі" знають, яку вигоду це їм принесе (підвищення по службі, передачу частини технічної роботи новому співробітникові, премію за наставництво).

Якщо за професійними якостями працівник відповідає своєму робочому місцю і робота на підприємстві задовольняє його потреби, такий працівник буде віддавати своєму підприємству максимум своїх сил, знань і здібностей. Він буде заробляти для підприємства набагато більше, ніж підприємство витратить на нього й організацію його роботи. Але врахувати особливості й індивідуальність кожного працівника підприємства - дуже і дуже складна задача.

Саме для рішення подібного роду питань виник кадровий консалтінг. *Кадровий консалтінг* - це система організаційно-психологічних заходів щодо діагностики і, за необхідністю, корекції організаційної структури і/або культури підприємства (організації) з метою поліпшення виробничих показників, оптимізації соціально-психологічного клімату, посилення мотивації персоналу.

Щоб підприємство працювало чітко і злагоджено, щоб фахівці віддавали роботі максимум сил і здібностей, де треба чітко виконували вказівки, а де – виявляли творчий підхід до справи і залишалися вірні своєму підприємству, потрібно, щоб підприємство задовольняло їх потреби. Відповідно, щоб підприємство було зацікавлене в задоволенні потреб працівника, необхідно, щоб і він задовольняв потреби підприємства. Ці позиції розглянуто в табл. 1.

Забезпечення інформаційної безпеки - багатогранна проблема, і робота з людьми є одною з найбільш складних ділянок. Як і раніше справедливе стародавнє гасло "Кадри вирішують все!", оскільки без надійних, високопрофесійних, відданих своїй організації кадрів, без згуртованого колективу забезпечити захист інформації неможливо. Діяльність служби персоналу повинна розглядатися як один з ключових елементів системи інформаційної безпеки підприємства.

Таблиця 1 – Кадровий консалтінг

Потреби підприємства відносно працівника	Потреби працівника відносно підприємства
Працівник повинен заробляти для підприємства грошей більше, ніж витрачається на його заробітну плату.	Підприємство повинно забезпечити збалансоване сполучення матеріальних та моральних складових мотивації працівника.
Працівник повинен робити точно те, що йому запропоновано посадовою інструкцією.	Підприємство повинно забезпечити працівникові визначений ступінь психологічного комфорту (це дуже багатофакторна вимога).
Працівник повинен бути адекватно ініціативний, у потрібний час використовувати творчий підхід до реалізації своїх функцій.	Працівник прагне до мінімізації витрат своєї праці.
Працівник повинен вміти в нестандартній ситуації прийняти і реалізувати оптимальне рішення.	

Висновки

У статті розроблено організаційні рекомендації управління персоналом системи інформаційної безпеки, наведено організаційно-психологічні заходи забезпечення інформаційної безпеки підприємства та розглядається взаємозв’язок робітника і організації. Українські підприємства повинні змінювати своє відношення до «людського фактору» і впроваджувати сучасні методи роботи з персоналом. Напрями

подальшої роботи у цій області будуть пов'язані з активним використанням значного потенціалу методів психоаналізу, психології й етики управління, конфліктології та ряду інших наук і більш повного інтегрування відповідних фахівців в управлінні системою інформаційної безпеки.

*Література: **1**. Стеклов В. К., Кільчицький Є. В. Основи управління мережами та послугами телекомунікацій. К.: „Техніка", 2002. - с. 84-86. **2**. Гафт М. Г. Методы оценки технического уровня, Интерактивный подход. //Проблемы информационных систем. – М.: № 2, 1987. – с. 11 – 21. **3**. Черноруцкий И. Г. Методы оптимизации и принятия решений. С.-Пб, 2001, с. 24. **4**. Микола Тардаскін, Володимир Кононович, Тетяна Тардаскіна. Аналіз інформаційної безпеки центрів обробки викликів. // „Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 8, 2004. С.140-146. **5**. Микола Тардаскін, Володимир Кононович, Тетяна Тардаскіна. Аналіз проблеми розподілу витрат на інформаційну безпеку інформаційно-телекомунікацйних систем. // „Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 8, 2004. С.62-68. **6**. Володимир Кононович, Тетяна Тардаскіна. Алгоритм розподілу ресурсів інформаційної безпеки документальних телекомунікацій. // „Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип.9, 2004. С. 152-161. 7. Тардаскін М. Ф. Особливості стратегії інформаційної безпеки цифрових автоматичних телефонних станцій // Зв'язок. – 2005. - № 1. – С. 31-33. **8.** Стандарт ISO 17779 "Обеспечение информационной безопасности организаций". **9.** Конституція України: Прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 р. – К.: Парламент, вид-во, 1999. – 95 с. **10.** Брединский А. Люди - источник конфиденциальной информации. Защита информации. Конфидент. 2004. - № 1 - с. 32-35. **11**. Копейкин Г. К., Лапина Н. А. Психологические аспекты информационной безопасности организации. Защита информации. Конфидент. 2003. - № 3 - с. 35. **12.** Микола Браіловський, Володимир Дорошко. Підготовка фахівців з інформаційної безпеки для підрозділів органів внутрішніх справ. // „Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", вип. 8, 2004. С.154-159.*

УДК 351.741:004.985

СТРАТЕГИЧЕСКОЕ ПЛАНИРОВАНИЕ ПРОЦЕССОВ ИНФОРМАТИЗАЦИИ И ПРИНЦИПЫ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ УКРАИНЫ

Павел Орлов, Николай Логвиненко, Владимир Торяник
Национальный университет внутренних дел

Аннотация: **Проведен системный анализ процессов информатизации общества и разработаны основные принципы стратегического планирования и управления информатизацией органов внутренних дел (ОВД) Украины.**
Summary: **The systems analysis of society informatization processes and developed basic principles of the strategic planning and management by informatization of Ukraine Internal Affairs were given.**
Ключові слова: **Информатизация ОВД, стратегическое планирование, информационное управление, інформационное общество.**

Введение

В связи с переходом человеческой цивилизации в постиндустриальную информационную эпоху информатизацию [1] в национальном масштабе следует рассматривать как важнейшую задачу любого современного государства. Экономическое и духовное развитие общества этой эпохи направляется на всестороннее гармоническое развитие личности. Человек, его творческие способности и потребности ставятся в центр современного демократического общества. Гармоничное развитие личности немыслимо без свободного и своевременного доступа к информации, современного информационного сервиса. Интеграция всех слоев населения в информационное общество, организация широкой доступности населения к информации становится важной политической задачей любого современного государства [1, 2].

К основным особенностям информационного общества относятся [3, 4]:

- сокращение количества занятых в промышленности и сельском хозяйстве за счет внедрения безлюдных технологий и робототехники, глобальное перераспределение рабочей силы, тотальное повышение образовательного уровня населения;