7. Конончук С. «Сильний» президент. Ще сильніший / С. Конончук [Електронний ресурс]. – Режим доступу : http://www.pravda.com.ua/articles/2012/05/21/6964926/view_print/

8. Жебрівський П. Навіть бюджетний комітет не все бачить / П. Жебрівський [Електронний ресурс]. – Режим доступу : http://www.epravda.com.ua/publications/2012/05/27/324791/view_print/

9. Послання Президента не варто робити основою для проекту бюджету [Електронний ресурс]. – Режим доступу : http://razumkov.org.ua/ukr/journal.php/files/category_journal/expert.php?news_id=3509

10. Берназюк Я. Повноваження Президента України в бюджетному процесі / Я. Берназюк // Публічне право. – 2014. – № 1 (13). – С. 19–27.

11. Про відмову у відкритті конституційного провадження у справі за конституційним поданням Кабінету Міністрів України щодо офіційного тлумачення положення пункту 30 частини першої статті 106 Конституції України від 30 травня 2007 року № 26 : Ухвала Конституційного Суду України [Електронний ресурс]. – Режим доступу : http://zakon0.rada.gov.ua/rada/show/v026u710-07

12. Про затвердження Положення про Міністерство фінансів України : Постанова Кабінету Міністрів України від 20 серпня 2014 року № 375 [Електронний ресурс]. – Режим доступу : http://zakon1.rada.gov.ua/laws/show/375-2014-п/paran8#n8

УДК 351.74

ЗАХИСТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ОБ'ЄКТА ЗАБЕЗПЕЧЕННЯ В ДІЯЛЬНОСТІ ПОЛІЦІЇ

AS PROTECTION OF INFORMATION SECURITY FACILITY SECURITY IN THE ACTIVITIES OF THE POLICE

Руколайніна І.Є.,
к.ю.н, доцент, доцент кафедри адміністративної діяльності ОВС
Харківський національний університет внутрішніх справ

Стаття присвячена захисту інформаційної безпеки як об'єкта забезпечення в діяльності поліції, виявленню факторів, які спричиняють негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації в поліції. Надано визначення терміну «комп'ютерна безпека» як еквівалента або замінника «інформаційної безпеки».

Ключові слова: інформація, інформаційна безпека, захист інформації, інформаційна система, суб'єкт інформаційних відносин, комп'ютерна безпека.

Статья посвящена защите информационной безопасности как объекта обеспечения в деятельности полиции, выявлению факторов, которые создают негативное информационное влияние, негативные последствия использования информационных технологий, несанкционированное распространение, использование и нарушение целостности, конфиденциальности и доступности информации. Дано определение термина «компьютерная безопасность» как эквивалента или заменителя «информационной безопасности».

Ключевые слова: информация, информационная безопасность, защита информации, информационная система, субъкт информационных отношений, компьютерная безопасность.

The article is devoted to the protection of information security as the security object in relation to policing, to identify factors that have negative information impact; negative consequences of using information technologies; unauthorized rospace, use, and violation of the integrity, confidentiality and availability of information to the police, we give a definition of the term «computer security» as an equivalent or substitute for «information security». The notion of «information» today is used very widely and versatile. It is difficult to find such a field of knowledge where it has not been used. Huge information flows literally overwhelm people. The volume of scientific knowledge, according to experts, doubling every five years. Information – information about people, objects, facts, events, phenomena and processes regardless the form of presentation.

Key words: information, information security, information protection, information system, subject of information relations, computer security.

Поняття «інформація» сьогодні вживається дуже широко і різнобічно. Важко знайти таку область знань, де б воно не використовувалося. Обсяг наукових знань, за оцінкою фахівців, подвоюється кожні п'ять років. Що ж таке інформація? Інформація – це дані про людей, предмети, факти, події, явища і процеси незалежно від форми їхнього представлення. Відомо, що інформація може мати різну форму, зокрема, дані, закладені в комп'ютерах, листи, пам'ятні записи, досьє, формули, креслення, діаграми, моделі продукції і прототипи, дисертації, судові документи тощо. Як і будь-який продукт, інформація має споживачів, що потребують її, і тому володіє певними споживчими якостями, а також має і своїх власників або виробників.

Термін «інформаційна безпека» розглядається в різних контекстах, і може мати різне змістовне наповнення. Під інформаційною безпекою (далі – ІБ) слід розуміти захист інтересів суб'єктів інформаційних відносин. ІБ як об'єкт забезпечення органами внутрішніх справ – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації. Закон України «Про інформацію» закладає основи правового забезпечення всіх найважливіших компонентів інформаційної діяльності: інформації й інформаційних систем; суб'єктів – учасників інформаційних процесів; 3) правовідносин виробників – споживачів інформаційної продукції; 4) власників (власників, джерел) інформації – оброблювачів і споживачів на основі відносин власності при забезпеченні гарантій інтересів громадян і держави.

Наша увага повинна бути зосереджена на зберіганні, обробці і передачі інформації незалежно від того, на якій мові (українській або іншій) вона закодована, хто або що є її джерелом і яку психологічну дію вона спричиняє на людей. Тому термін «інформаційна безпека» використовуватиметься у вузькому сенсі, так, як це прийнято, наприклад, в англомовній літературі.

Під ІБ ми розуміємо захищеність інформації та інфраструктури, що її підтримує, від випадкових або навмисних

дій природного або штучного характеру, які можуть завдати неприємного збитку суб'єктам інформаційних відносин, зокрема власникам і користувачам інформації та інфраструктури, що її підтримує. Захист інформації – це комплекс заходів, направлених на забезпечення ІБ. Таким чином, правильний з методологічної точки зору підхід до проблем ІБ починається з виявлення суб'єктів інформаційних відносин та інтересів цих суб'єктів, пов'язаних з використанням інформаційних систем (далі – ІС). Загроза ІБ – це зворотна сторона використання інформаційних технологій. Тут необхідно зауважити, що трактування проблем, пов'язаних з ІБ, для різних категорій суб'єктів може істотно різнитися. Отже, ІБ не зводиться виключно до захисту від несанкціонованого доступу (далі – НСД) до інформації, це принципово ширше поняття. Суб'єкт інформаційних відносин може постраждати (зазнати збитки та/або одержати моральний збиток) не тільки від НСД, але й від поломки системи, що викликала перерву в роботі. Більш того, для багатьох відкритих організацій власне захист від НСД до інформації стоїть за важливістю не на першому місці.

Повертаючись до питань термінології, відзначимо, що термін «комп'ютерна безпека» (як еквівалент або замінник ІБ) важається нам дуже вузьким. Комп'ютери – тільки одна із складових ІС, і хоча наша увага буде зосереджена, в першу чергу, на інформації, яка зберігається, обробляється і передається за допомогою комп'ютерів, її безпека визначається всією сукупністю складових і, в першу чергу, найслабкішою ланкою, якою в переважній більшості випадків виявляється людина. Згідно визначення ІБ, вона залежить не тільки від комп'ютерів, але і від інфраструктури, що її підтримує, до якої можна віднести системи електро-, водо– і теплопостачання, кондиціонери, засоби комунікацій і, звичайно, обслуговуючий персонал. Ця інфраструктура має самостійну цінність, але нас цікавитиме лише те, як вона впливає на виконання своїх функцій в діяльності поліції.

Забезпечення ІБ у діяльності поліції – багатогранна, можна навіть сказати, багатовимірна область діяльності, в якій успіх може принести тільки систематичний, комплексний підхід. Спектр інтересів суб'єктів, пов'язаних з використанням ІС, можна розділити на наступні категорії: забезпечення доступності, цілісності і конфіденційності інформаційних ресурсів та інфраструктури, що її підтримує.

Доступність – це можливість за прийнятний час одержати необхідну інформаційну послугу. ІС створюються для отримання певних інформаційних послуг. Якщо з тих або інших причин надати ці послуги користувачам стає неможливо, то очевидно, що це завдасть збитку всім суб'єктам інформаційних відносин. Тому, не протиставляючи доступність решті аспектів, ми виділяємо її як найважливіший елемент ІБ.

Цілісністю є актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованої зміни. Цілісність можна поділити на статичну (тобто незмінність інформаційних об'єктів) і динамічну (що відноситься до коректного виконання складних дій (транзакцій). Засоби контролю динамічної цілісності застосовуються, зокрема, при аналізі потоку фінансових повідомлень з метою виявлення крадіжки, переупорядковування або дублювання окремих повідомлень. Цілісність є найважливішим аспектом ІБ в тих випадках, коли інформація служить «керівництвом до дії». Рецепт ліків, характеристики комплектуючих виробів, хід технологічного процесу – все це приклади інформації, порушення цілісності якої може опинитися в буквальному розумінні смертельним. Неприємно і спотворення офіційної інформації, чи то тексту закону, чи сторінки Web-сервера якої-небудь організації.

Конфіденційність – це захист від НСД до інформації. Конфіденційність – найбільш опрацьований в нашій країні аспект ІБ. На жаль, практична реалізація заходів по забезпеченню конфіденційності сучасних ІС натрапляє на серйозні перепони. По-перше, відомості про технічні канали просочування інформації є закритими, а, отже, більшість користувачів позбавлена можливості скласти уявлення про потенційні ризики. По-друге, на шляху призначеної для користувача криптографії як основного засобу забезпечення конфіденційності стоять численні законодавчі перепони і технічні проблеми. Нарешті, конфіденційні моменти є також у багатьох організацій (навіть в учбових закладах прагнуть не розголошувати дані про екзаменаційні білети до іспиту).

ІБ є одним з найважливіших аспектів інтегральної безпеки, на якому б рівні ми не розглядали останню – національному, галузевому, корпоративному або персональному. Прикладом є історія про одну студентку яка втратила стипендію у 18 тисяч доларів в Мічиганському університеті через те, що її сусідка по кімнаті скористалася їх загальним системним входом і відправила від імені своєї жертви електронний лист з відмовою від стипендії. При аналізі проблематики, пов'язаної з ІБ, необхідно зважати на специфіку даного аспекту безпеки, що полягає в тому, що ІБ є складовою частиною інформаційних технологій – області, що розвивається безпрецедентно високими темпами. На жаль, сучасна технологія програмування не дозволяє створювати безпомилкові програми, що не сприяє швидкому розвитку засобів забезпечення ІБ. У принципі, це можливо, але вимагає дотримання певних принципів і контролю за станом захищеності на протязі життєвого циклу ІС. У таких умовах системи ІБ повинні уміти протистояти різноманітним атакам, як зовнішнім, так і внутрішнім, атакам автоматизованим і скоординованим. Іноді напад триває долі секунди; деколи поволі і розтягується на години, так що підозріла активність практично непомітна. Метою зловмисників може бути порушення всіх складових ІБ – доступності, цілісності або конфіденційності.

На нашу думку, потрібно структурувати засоби ІБ. Введемо наступні види забезпечення ІБ в діяльності поліції:

– законодавчі заходи забезпечення ІБ;

– адміністративні заходи (накази, нормативно-правові акти і інші дії керівництва поліції, пов'язані з ІС, що захищаються);

– процедурні заходи (заходи безпеки, орієнтовані на людей);

– програмно-технічні заходи.

Закони і нормативні акти орієнтовані на всіх суб'єктів інформаційних відносин незалежно від їх організаційної приналежності (це можуть бути як юридичні, так і фізичні особи) в межах країни (міжнародні конвенції мають навіть ширшу область дії), адміністративні заходи – на всіх суб'єктів в межах організації, процедурні – на окремих людей (або невеликі категорії суб'єктів), програмно-технічні – на устаткування і програмне забезпечення.

Система ІБ в поліції України базується на законах України «Про інформацію» [1], «Про державну таємницю» [2], «Про національну програму інформатизації» [3], «Про доступ до публічної інформації» [4] тощо. Крім того, при побудові системи ІБ слід враховувати зміст відповідних статей Кримінального та інших кодексів України, норм Положення про забезпечення режиму таємності під час обробки інформації, що становить державну таємницю, в автоматизованих системах, затверджене Постановою Кабінету Міністрів України від 16 лютого 1998 року № 180, Постанови Кабінету Міністрів України «Про затвердження Концепції технічного захисту інформації в Україні» від 08 листопада 1997 року № 1126, наказів Міністерства внутрішніх справ України «Про організацію і виконання робіт з технічного захисту інформації з обмеженим доступом в системі МВС України» від 14 липня 1998 року, «Про заходи щодо забезпечення вимог Закону України «Про внесення змін і доповнень в Закон про дер-

жавну таємницю» від 31 жовтня 1999 року № 860, інших наказів Міністерства внутрішніх справ України, а також – наказів Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України.

Система ІБ спрямована на запобігання втраті інформації, її спотворенню, НСД та незаконному її використанню на етапах проектування, впровадження та експлуатації інформаційних підсистем. В експлуатаційному режимі програмно-технічні комплекси повинні забезпечити ефективне і надійне функціонування інформаційних підсистем та захист від НСД.

Основною метою системи захисту інформації в поліції є:

– фізичне збереження технічних і програмних засобів від викрадення та пошкодження;

– надання користувачам права доступу до ресурсів підсистеми згідно з прийнятою стратегією безпеки;

– забезпечення входу до комп'ютерної підсистеми за умови пред'явлення електронного ідентифікатора або вводу особистого паролю;

– реєстрація дій користувачів щодо ресурсів підсистеми;

– забезпечення цілісності інформаційних ресурсів (у тому числі – забезпечення антивірусного захисту);

– облік носіїв інформації;

– сигналізація про порушення захисту;

– забезпечення цілісності програмних засобів та інформації, що обробляється.

Підсистема контролю доступу і захисту інформації повинна реалізовувати основні методи захисту інформаційних ресурсів від НСД, а також забезпечувати нейтралізацію випадкових і цілеспрямованих потенційних загроз, таких, що дають змогу порушнику:

– одержувати доступ до даних з порушенням встановлених правил розмежування доступу з метою ознайомлення, модифікації, копіювання, знищення даних і т. ін.;

– зчитувати дані із запам'ятовуючих пристроїв після виконання санкціонованих запитів;

– копіювати носії інформації;

– маскуватися під зареєстрованого користувача, видавати власні несанкціоновані запити за запити операційної системи;

– отримувати захищені дані за допомогою спеціально організованої серії санкціонованих запитів;

– модифікувати програмне забезпечення, навмисно включаючи до його складу спеціальні блоки для порушення безпеки даних;

– фальсифікувати факти формування, видачі та отримання даних;

– підтверджувати отримання від користувача даних, сформованих самим порушником,

– передавати користувачеві дані, що не передавалися;

– вивчати права доступу інших користувачів;

– незаконно розширювати свої права та змінювати повноваження інших користувачів.

При захисті комп'ютерних систем від НСД треба враховувати специфіку їх використання. Як правило, окремим комп'ютером користується обмежена кількість користувачів. ПК можуть функціонувати як в автономному режимі, так і у складі локальних мереж, підключатися до глобальної мережі Internet тощо.

Для захисту ПК від НСД використовуються різноманітні програмні засоби, серед яких найбільше розповсюдження отримали:

– засоби захисту обчислювальних ресурсів (використовують парольну ідентифікацію);

– застосування різноманітних методів шифрування інформації;

– засоби захисту від копіювання комерційних програм;

– захист від комп'ютерних вірусів та ін.

Засоби парольної ідентифікації. Можна використати апаратні засоби встановлення паролю на запуск операційної системи за допомогою установок в CMOS Setup. Однак, використання такої парольної ідентифікації не є надійним, для подолання такого захисту достатньо, наприклад, ввести універсальний пароль (AWARD_SW) або відключити акумуляторну батарею комп'ютера.

Захист накопичувача на жорсткому магнітному диску. Існує декілька видів програмних засобів для вирішення цього завдання: захист від будь-якого доступу до жорсткого диску; захист диску від запису і читання; контроль за зверненнями до диска; засоби видалення залишків конфіденційної інформації. Як правило, застосування таких методів дозволяє надійно захистити жорсткий диск від НСД.

Криптографічний захист інформації – це спеціальні методи перетворення інформації, в результаті якого вона стає недоступною без пред'явлення ключа і зворотного перетворення. Криптографічний метод захисту інформації вважається найбільш надійнішим (охороняється сама інформація, а не доступ до неї). Цей метод захисту реалізується шляхом застосування пакетів програм, що розширюють можливості операційної системи.

Сьогодні поки не існує загально визнаної класифікації криптографічних методів захисту інформації. Проте, коли шифрується кожний символ повідомлення (симетричний метод закриття інформації), можна умовно виділити чотири основні групи: підстановка – символи тексту, що шифрується, заміняються символами того ж або іншого алфавіту (за визначеним правилом); перестановка – символи тексту переставляються за певним правилом у межах заданого блоку тексту; аналітичне перетворення – текст перетворюється за певним аналітичним правилом; комбіноване перетворення – текст шифрується декількома засобами шифрування.

Існує значна кількість програмних засобів для шифрування інформації, що різняться за ступенем надійності. Слід відзначити, що жодна система захисту даних не може вважатися надійною. Тому, зокрема в імені пароля, не можна використовувати очевидні фрази, які легко вгадати. Злом системи захисту злочинці можуть здійснювати, зокрема, шляхом підробки відкритих ключів, аналізу видалених (не до кінця) файлів, а також файлів підкачки (віртуальна пам'ять), створювання комп'ютерних вірусів чи програмних закладок [5].

Крім того, порушення режиму фізичного доступу може дозволити сторонній особі захопити файли з вихідним текстом. Методи криптографії захищають дані тільки доти, доки вони зашифровані, і не можуть перешкодити порушенню режиму фізичної безпеки, коли розкритою може стати текстова або звукова інформація (цей вид атак простіше і дешевше, ніж криптоаналіз).

Технічно добре оснащеними злочинцями може бути вчинена атака ще одного виду, що полягає у віддаленому перехопленні побічного електромагнітного випромінювання і наводок (ПЕВІН) від комп'ютера. Так, спеціальне обладнання може перехоплювати інформацію, що відображається на дисплеї комп'ютера на відстані до 1 тис. метрів. Цей потенційний канал витоку інформації можна захистити шляхом екранування комп'ютерного обладнання і мережних кабелів. Така технологія відома з назвою Tempest і застосовується урядовими і оборонними організаціями. Крім того, можна використовувати спеціальні генератори шуму («ГБШ-1», «Салют», «Пелена», «Грім», «Волна» та ін.).

Існує також проблема захисту від неправильних дат в електронному підписі. Слід враховувати, що іноді «некоректна» дата поруч із підписом не є шахрайством. У ситуаціях, коли виникає питання про те, що підпис на звичайному паперовому документі виконаний саме у визначений час, звертаються до нотаріуса, який засвідчує момент підпису і завіряє це своїм підписом. Аналогічно, при використанні цифрового підпису для завірення дати підпису документа можна звернутися до третьої сторони, яка користується довірою, щоб вона сертифікувала підпис.

Захист паролем документів MS-Office. Фахівці не рекомендують використовувати цей метод, злом настільки простий, що на це витрачається лише кілька секунд. Найчастіше зламуються документи MS Word і MS Excel.

Захист даних за допомогою програми «Кобра». Дану програму навіть закордонні фахівці вважають найдосконалішою криптосистемою.

Програмою інформатизації поліції України передбачено ряд заходів стосовно інформатизації оперативно-розшукової діяльності в поліції. Зокрема, впровадження типової інформаційної підсистеми (далі – ІПС) «Розшук» з обліку осіб, оголошених в регіональний, державний (міждержавний) розшук, ІПС «Повідомлення», «Оріон» та «Пізнання» тощо [6]. Крім того, програмою передбачено заходи щодо розвитку засобів комп'ютерного обміну інформацією та поширення мережі користувачів ІПС, розробки проекту використання мережі Internet в органах внутрішніх справ України.

Враховуючи, що у більшості ІПС обробляється інформація з обмеженим доступом, розробляється концепція комплексного захисту ІС в Україні, визначаються спеціальні вимоги до засобів комп'ютерної техніки, передачі даних та криптографічних засобів, ведуться роботи з атестування, видачі ліцензій комп'ютерних мереж та автоматизованих робочих місць, де обробляється інформація з обмеженим доступом. Вимоги до надійності та ІБ інформаційно-пошукових систем викладено в проекті створення інформаційно-аналітичної системи поліції України. Відмічається, що безпека і захист ІС має будуватись з урахуванням комплексного підходу до структури системи захисту, що передбачає об'єднання в єдиний комплекс відповідних заходів та засобів захисту інформації на всіх рівнях системи інформаційного забезпечення.

ЛІТЕРАТУРА

1. Про інформацію : Закон України від 02 жовтня 1992 року № 2657-XII // Відомості Верховної Ради України. – 1992. – № 48. – Ст. 650.

2. Про державну таємницю : Закон України від 21 січня 1994 року № 3855-XII // Відомості Верховної Ради України. – 1994. – № 16. – Ст. 93.

3. Про національну програму інформатизації : Закон України від 16 жовтня 2012 року № 5463-VI // Відомості Верховної Ради України. – 2012. – № 14. – Ст. 83.

4. Про доступ до публічної інформації : Закон України від 13 січня 2011 року № 2939-VI // Відомості Верховної Ради України. – 2011. – № 32. – Ст. 314.

5. Токар О. І. Державна інформаційна політика : проблеми визначення концепту / О. І. Токар // Політ. менеджмент. – 2009. – № 5. – С. 131–141.

6. Кукшинова О. О. Правове регулювання доступу до відкритої інформації : Дис. ... канд. юрид. наук за спец. : 12.00.07 / О. О. Кукшинова ; НАН України, Ін-т держави і права ім. В. М. Корецького. – К., 2012. – 211 с.

УДК 342.97:65.01

ДІАГНОСТИКА РОБОТИ КЕРІВНИЦТВА ПІДПРИЄМСТВА НА ІНСТИТУЦІЙНОМУ РІВНІ УПРАВЛІННЯ В КОНТЕКСТІ ДОТРИМАННЯ ЧИННОГО ЗАКОНОДАВСТВА, СТАТУТУ ТА ВИКОНАННЯ ПОСАДОВИХ ОБОВ'ЯЗКІВ

DIAGNOSTICS OF THE ENTERPRISE EXECUTIVES' ACTIVITIES AT THE INSTITUTIONAL LEVEL OF GOVERNANCE IN THE CONTEXT OF THE APPLICABLE LEGISLATION, STATUTE AND FULFILLMENT OF THE OFFICIAL DUTIES

Скриньковський Р.М.,
к.е.н., доцент кафедри економіки підприємств та інформаційних технологій
ПВНЗ «Львівський університет бізнесу та права»

Крамар Р.І.,
к.ю.н., доцент, доцент кафедри цивільно-правових дисциплін
ПВНЗ «Львівський університет бізнесу та права»

У статті розкрито сутність керівництва підприємства на інституційному рівні управління, під яким слід розуміти головного керівника (або керівника вищої ланки управління), а також його заступників, які реалізують функції менеджменту (контролювання, планування, дія та/або делегування), розробляють методи менеджменту (економічні, адміністративні, технологічні тощо), приймають управлінські рішення (перспективні, поточні) в системі «інформація – ресурс – час», що, враховуючи думку Лауреата Нобелівської премії 1976 року, Мілтона Фрідмана, спрямовані на розвиток підприємства та формування його перспективи (через збільшення прибутку, частки ринку тощо) на умовах виконання правил гри (законодавчих актів, чесного слова, без обману і шахрайства тощо) та участі у конкурентній боротьбі. Розглянуто правовий статус головного керівника підприємства, що відображає його права і обов'язки, а також юридичне гарантування його прав як суб'єкта трудових правовідносин.

Ключові слова: підприємство, керівництво, діагностика, правовий статус керівника, юридична відповідальність.

В статье раскрыта сущность руководства предприятия на институциональном уровне управления, под которым следует понимать главного руководителя (или руководителя высшего звена управления), а также его заместителей, которые реализуют функции менеджмента (контроль, планирование, действие и/или делегирование), разрабатывают методы менеджмента (экономические, административные, технологические и т.д.), принимают управленческие решения (перспективные, текущие) в системе «информация – ресурс – время», что, учитывая мнение Лауреата Нобелевской премии 1976 года, Милтона Фридмана, направлены на развитие предприятия и формирование его перспективы (путем увеличения прибыли, доли рынка и т.п.) на условиях выполнения правил игры (законодательных актов, честного слова, без обмана и мошенничества и т.д.) и участия в конкурентной борьбе. Рассмотрен правовой статус главного руководителя предприятия, отражающий его права и обязанности, а также юридическое обеспечение прав как субъекта трудовых правоотношений.

Ключевые слова: предприятие, руководство, диагностика, правовой статус руководителя, юридическая ответственность.