УДК 342.951:65.01

ДІАГНОСТИКА ЕФЕКТИВНОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ ТА ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО КОМЕРЦІЙНУ ТАЄМНИЦЮ

DIAGNOSTIC OF INFORMATION SECURITY EFFICIENCY AT ENTERPRISE AND RESPONSIBLE FOR VIOLATION OF COMMERCIAL SECRECY LEGISLATION

Скриньковський Р.М.,
кандидат економічних наук, доцент кафедри економіки підприємств та інформаційних технологій Львівського університету бізнесу та права, помічник-консультант депутата Львівської обласної ради

Крамар Р.І.,
кандидат юридичних наук, доцент кафедри цивільно-правових дисциплін Львівського університету бізнесу та права

Гарасим П.С.,
кандидат юридичних наук, доцент кафедри кримінально-правових дисциплін Львівського державного університету внутрішніх справ, начальник залізничного відділу поліції Головного управління Національної поліції у Львівській області

У статті розкрита сутність діагностики ефективності системи захисту інформації на підприємстві. Встановлено, що ключовими бізнес-індикаторами діагностики ефективності системи захисту інформації на підприємстві є: рівень цінності інформації; рівень секретності інформації; рівень доступності до інформації; рівень контролю за захистом інформації; частота і вагомість діяння щодо порушення захисту інформації. З'ясовано, що внаслідок порушення законодавства України про інформацію до винних може застосовуватись дисциплінарна, матеріальна, цивільно-правова, адміністративна та кримінальна відповідальність.

Ключові слова: підприємство, інформація, комерційна таємниця, юридична відповідальність, діагностика.

В статье раскрыта сущность диагностики эффективности системы защиты информации на предприятии. Установлено, что ключевыми бизнес-индикаторами диагностики эффективности системы защиты информации на предприятии являются: уровень ценности информации; уровень секретности информации; уровень доступности к информации; уровень контроля за защитой информации; частота и значимость деяния о нарушении защиты информации. Выяснено, что в результате нарушения законодательства Украины об информации к виновным может применяться дисциплинарная, материальная, гражданско-правовая, административная и уголовная ответственность.

Ключевые слова: предприятие, информация, коммерческая тайна, юридическая ответственность, диагностика.

The article reveals essence of diagnostic of information security efficiency at enterprise. It is been determined that key business indicators of diagnostic of information security efficiency at enterprise are: level of information value; level of information classification; level of information accessibility; level of control of information security; the frequency and significance of act of violation of information security. It has been ascertained that violation of Information Legislation of Ukraine may result in disciplinary, financial, civil law, administrative and criminal responsibility.

Key words: enterprise, information, commercial secrecy, legal responsibility, diagnostics.

Актуальність теми. В основі забезпечення результативного розвитку підприємства (суб'єкта господарювання) лежить взаємодія трьох складових: інформація, ресурс та час. Реалії сьогодення засвідчують появу фінансових махінацій та незаконних дій у сфері конкуренції на засадах неправомірного збирання, використання та розголошення інформації, що є конфіденційною.

Так, «2016 (рік), коли суспільство змушене покладатися на корпорацію *(Apple),* щоб захистити свої права. Це тривожний знак»). Таку думку 21.03.2016 р. у своєму мікроблозі Twitter висловив колишній співробітник американських спецслужб Е. Сноуден *(Edward J. Snowden),* відносно якого у США на початку червня 2013 р. заведено кримінальну справу за передачу газетам *«The Guardian» і «The Washington Post»* секретної інформації Агентства нацбезпеки США, включаючи про проект PRISM, X-Keyscore і Tempora. «Компаніям, які не розуміють можливих ризиків, краще не користуватися хмарними технологіями» (аналітик IDC Ф. Хочмас *(Phil Hochmuth)*). Звідси очевидно, що бізнесу та приватним користувачам варто замислитись над рівнем безпеки в середовищі хмарних технологій.

Поряд із тим 12.03.2016 р. Українське національне інформаційне агентство «Укрінформ» повідомляє, що президент США Б. Обама *(Barack H. Obama)* напередодні у п'ятницю під час виступу в американському штаті Техас не став коментувати протистояння ФБР та *Apple,* проте пояснив, чому від держави не повинно бути таємниць. За словами американського лідера, це, зокрема, ускладнило би боротьбу з незаконним ухиленням від сплати податків або фінансовими аферами. В контексті цього зазначимо: 03.04.2016 р. Міжнародний консорціум журналістських розслідувань *(ICIJ)* та Центр з дослідження корупції та організованої злочинності *(OCCRP)* в рамках проекту «Панамський архів» *(Panama Papers)* опублікували масштабне розслідування про причетність окремих світових лідерів та політиків до ухилення від сплати податків, корупції, відмивання грошей та інших фінансових махінацій з використанням офшорних схем. Тут коментарі зайві.

Звідси очевидно, що важливого значення в даний час набуває ідентифікування, аналіз та оцінювання ефективності системи захисту інформації на підприємстві з метою усунення перешкод щодо порушення законодавства про комерційну таємницю.

Основні (ключові) аспекти захисту інформації на підприємстві регулюються нормами таких законодавчих та нормативно-правових документів, як Закон України «Про

інформацію», Цивільний кодекс України, постанова Кабінету Міністрів України «Про перелік відомостей, що не становлять комерційної таємниці», Господарський кодекс України, Кодекс законів про працю України, Кодекс України про адміністративні правопорушення, Кримінальний кодекс України [1–7].

Вагомий внесок у розвиток нормативно-правового та методологічного забезпечення захисту інформації на підприємстві, що становить його комерційну таємницю, зробили такі вітчизняні науковці та практики, як Т.В. Боцян, А.І. Берлач, І.І. Килимник, П.Є. Матвієнко, Н.Д. Махновська, Ю.В. Носік, О.Е. Радутний, Г.О. Сляднєва, Н.П. Спільна, О.В. Харитонов, С.О. Харламова, О.В. Черевко, Л.Г. Чистоклетов та ін. [8–18].

Водночас, як свідчать результати аналізу наукових праць [8–18] та законодавчої та нормативно-правової бази України [1–7], не до кінця вивченими залишаються питання діагностики ефективності системи захисту інформації на підприємстві.

Метою наукової роботи є формування концептуальних засад діагностики ефективності системи захисту інформації на підприємстві з урахуванням відповідальності за порушення законодавства про комерційну таємницю.

Виклад основного матеріалу дослідження. В контексті зазначеного вище першочергово виникає потреба в розкритті сутності понять «інформація» та «комерційна таємниця».

Так, згідно з ч. 1 ст. 1 Закону України «Про інформацію» [1] інформація являє собою «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді».

Що стосується сутності поняття «комерційна таємниця», то у науковому дослідженні О.Е. Радутного [8] зазначено, що комерційна таємниця – це деякий обсяг інформації, яка знаходиться у власності фізичних чи юридичних осіб (суб'єктів господарювання), характеризується рисами економічної цінності, відокремленості і доступ до якої та використання якої проводиться у рамках спеціального правового режиму. На думку Г.О. Сляднєвої [9], комерційна таємниця – це комерційно цінна конфіденційна інформація, яка охороняється суб'єктом господарювання та доступ до якої є обмеженим задля захисту прав і законних інтересів власника цієї інформації.

Відповідно до ч. 1 ст. 505 Цивільного кодексу України (ЦКУ) [2], комерційна таємниця – це «інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних для існуючих обставин заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію» [2].

Результати аналізу наукової праці [10] дають підстави стверджувати, що інформація, будучи комерційною таємницею, повинна мати дійсну комерційну цінність та бути невідомою для третіх осіб.

Відповідно до ч. 1 ст. 420 ЦКУ [2] комерційна таємниця є одним із об'єктів права інтелектуальної власності.

До комерційної таємниці слід відносити відомості комерційного, виробничого, організаційного, технічного або іншого характеру, окрім тих, що згідно із законом, не можна віднести до комерційної таємниці (ч. 2 ст. 505 ЦКУ) [2].

Відповідно до постанови Кабінету Міністрів України «Про перелік відомостей, що не становлять комерційної таємниці» [3], до комерційної таємниці не відносять [3]: 1) установчі документи; документи, що надають дозвіл займатися господарською чи підприємницькою діяльністю, а також окремими її видами; 2) дані, що необхідні для розрахунку та оплати податків і інших обов'язкових платежів; 3) дані про склад і чисельність працюючих, отримувану ними заробітну плату як загалом, так і за посадами, професіями; наявність вільних робочих місць; 4) документи про оплату податків і інших обов'язкових платежів; 5) інформацію про забруднення навколишнього середовища, недотримання та незабезпечення безпечних умов праці; реалізацію продукції, яка шкодить здоров'ю; інші правопорушення чинного законодавства України і розміри збитків, що при цьому заподіяні; 6) документи про платоспроможність; 7) дані про участь посадових осіб підприємства у кооперативах, спілках, малих підприємствах, об'єднаннях та інших організаціях, що здійснюють підприємницьку діяльність; 8) дані (відомості), які відповідно до чинного законодавства України підлягають оголошенню.

У науковому дослідженні С.О. Харламової [11] зазначено, що комерційна таємниця характеризується такими особливостями [11]: спеціальне оформлення локальними актами; зміст та обсяг визначається керівництвом підприємства (установи, організації); є власністю підприємства, що здійснює її охорону; у будь-який момент відомості комерційної таємниці можуть бути розкриті підприємством-власником. Натомість науковець Ю.В. Носік [12] стверджує, що до основних ознак комерційної таємниці доцільно віднести інформаційність, конфіденційність, комерційну цінність і захищеність [12].

Разом із тим, згідно з ч. 1 ст. 162 Господарського кодексу України (ГКУ) [4] суб'єкт господарювання, в тому числі підприємство, є власником інформації технічного, організаційного або іншого комерційного характеру, має право захисту від незаконного використання третіми особами зазначеної вище інформації відповідно до умов, якщо ця інформація містить комерційну цінність, невідома третім особам та доступ до неї не є вільним на законодавчій основі. За таких умов власник інформації має повне право на вжиття належних заходів щодо охорони конфіденційності цієї інформації [4].

У ході дослідження праці Н.П. Спільної [13] з'ясовано, що основними правами власника на комерційну таємницю є [13]: право на використання комерційної таємниці; право дозволяти іншим особами використовувати комерційну таємницю; право здійснювати перешкоду неправомірному розповсюдженню комерційної таємниці, її збиранню чи використанню.

Щодо захисту інформації, то він становить цілісну сукупність адміністративних, правових, технічних, організаційних чи інших заходів щодо забезпечення збереження та цілісності інформації і створення належного порядку доступу до неї (ч. 1 ст. 1 Закону України «Про інформацію» [1].

Основними напрямами забезпечення комплексного захисту інформації на підприємстві, на думку проф. Н.П. Спільної та науковця Н.Д. Махновської [13], є [13, с. 122]: 1) фізичний захист інформації (полягає у використанні автоматизованих систем аналізування інформації з позиції фізичної захищеності та зберігання); 2) криптографічний захист інформації (передбачає шифрування інформації); 3) електромагнітний захист інформації (характеризує конфіденційність інформації з використанням електромагнітних полів); 4) економічний захист інформації (передбачає проведення економічних обчислень і обґрунтування доцільності захисту інформації відносно них); 5) активний захист інформації (полягає у розробленні активних заходів щодо створення перешкод до отримання доступу до інформації). В свою чергу, проф. А.І. Берлач [14] стверджує, що порушення системи заходів стосовно захисту комерційної таємниці (конфіденційної інформації) може спровокувати [14. с. 41]: зниження рівня економічної безпеки підприємства; послаблення відносин із діловими партнерами; розірвання договорів, контрактів; високий рівень плинності кваліфікованих кадрів; виникнення значних фінансових затрат; шкоду діяльності підприємства загалом.

Беручи до уваги вищезазначене, оформлення правового захисту комерційної таємниці на підприємстві передбачає ви-

конання таких основних завдань [15. с. 60]: визначення даних (відомостей), що відносяться до комерційної таємниці; забезпечення технічного захисту даних (відомостей); визначення осіб, що матимуть доступ (повний чи обмежений) до комерційної таємниці; організування роботи з документацією, в якій міститься комерційна таємниця; встановлення відповідальності осіб та слідкування за процесом її дотримання стосовно захисту інформації, що містить комерційну таємницю.

Що стосується зацікавлених осіб у витоку конфіденційної інформації про підприємство, то ними є [16]: підприємства-конкуренти; особи, що планують здійснювати аналогічну діяльність; співробітники підприємства через невдоволення своїм становищем на підприємстві; сторонні особи, що бажають заробити на продажі комерційної таємниці підприємствам-конкурентам; кримінальні структури.

Водночас до суб'єктів, що беруть участь у правовідносинах стосовно визначення, зберігання та розповсюдження комерційної таємниці, доцільно відносити [15, с. 40]: власників комерційної таємниці; посадових осіб органів державної влади, які здійснюють перевірку підприємств, установ, організацій; партнерів власників комерційної таємниці, що отримали доступ до комерційної таємниці за результатами укладення і виконання угод; працівників підприємства, що працюють згідно з трудовим договором.

Як показав аналіз літературного джерела [11], незаконні дії з інформацією, що становить комерційну таємницю, мають дві сторони. З позиції об'єктивної сторони − незаконні дії передбачають збирання інформації з ціллю її використання та розголошення. Щодо суб'єктів незаконних дій з даними комерційної таємниці, то ними можуть бути працівники підприємства та спеціальні особи, що здійснюють професійну чи службову діяльність [11].

У свою чергу предмет злочинів щодо комерційної таємниці характеризується такими ознаками [8]: 1) об'єктивністю існування комерційної таємниці (комерційна інформація, будучи одним із ресурсів, знаходиться поза межами свідомості людини); 2) таємністю (забезпечення спеціального режиму доступу до комерційної таємниці); 3) соціальною ознакою (взаємовідносини із суспільством щодо збереження комерційної таємниці); 4) юридичною ознакою (передбаченням у законодавстві предмета злочину).

З метою запобігання витоку конфіденційної інформації, на підприємстві повинна використовуватися система градації документів (за рівнем доступу). Так, на першому рівні доступу (обмеженому) внутрішні документи підприємства повинні містити спеціальний гриф «Для службового користування»; на другому – «Таємно», а на третьому – «Цілком таємно». Доступ до документів із зазначеними вище спеціальними грифами повинні мати спеціально-уповноважені працівники підприємства [16].

Таким чином, проведений аналіз наукових праць [1–17] та діючої практики в цьому напрямі дозволяє зробити висновок: 1) діагностика ефективності системи захисту інформації на підприємстві передбачає ідентифікування, аналізування і оцінювання рівня ефективності системи захисту інформації на підприємстві, основних тенденцій його зміни на засадах нормативно-правового та методологічного забезпечення діяльності підприємства з урахуванням безпеки в середовищі хмарних технологій; 2) ключовими бізнес-індикаторами системи діагностики ефективності системи захисту інформації на підприємстві є: рівень цінності інформації; рівень секретності інформації; рівень доступності до інформації; рівень контролю за захистом інформації; частота і вагомість діяння щодо порушення захисту інформації.

Згідно з ч. 1 ст. 27 Закону України «Про інформацію» [1] внаслідок порушення законодавства України про інформацію на винних може накладатися дисциплінарна, цивільно-правова, адміністративна чи кримінальна відповідальність.

Поряд із тим доцільно також враховувати такий вид відповідальності, як матеріальну, оскільки цей вид відповідальності, з урахуванням дисциплінарної, регулює трудові правопорушення на підприємстві.

Так, матеріальну відповідальність у розмірі не більше свого середньомісячного заробітку несуть працівники, за винятком працівників, які є посадовими особами, за шкоду, що заподіяна з їх вини підприємству (установі, організації) внаслідок виконання своїх трудових обов'язків (ст. 132 Кодексу законів про працю України (КЗпПУ) [5].

Адміністративна відповідальність щодо збереження комерційної таємниці регулюється Кодексом України про адміністративні правопорушення (КУпАП). Згідно зі ст. 1643 КУпАП [6] копіювання форми, зовнішнього оформлення, упаковки на незаконних підставах, а також імітування копіювання, однотипне відтворення товару іншого суб'єкта господарювання та/чи самовільне використання його імені передбачає накладення штрафу в розмірі від тридцяти до сорока чотирьох неоподаткованих мінімумів доходів громадян із конфіскуванням продукції, що вироблена, знарядь праці, сировини. За навмисне розповсюдження неправдивих чи неточних відомостей, що здатні завдати шкоди діловій репутації чи інтересам іншого суб'єкта господарювання, накладається штраф у розмірі від п'яти до дев'яти неоподаткованих мінімумів доходів громадян. Незаконне отримання, використання та розголошення комерційної таємниці (чи іншої конфіденційної інформації) з ціллю завдання шкоди діловій репутації чи інтересам іншого суб'єкта господарювання передбачає накладення штрафу від дев'яти до вісімнадцяти неоподаткованих мінімумів доходів громадян [6].

На думку П.Є. Матвієнко [10], визначальним об'єктом адміністративних правопорушень законодавства про комерційну таємницю слід вважати суспільні відносини щодо захисту суб'єктів господарювання від недобросовісної конкуренції [10].

Що стосується кримінальної відповідальності, то згідно зі ст. 231 Кримінального кодексу України (ККУ) [7] за умисні діяння щодо отримання відомостей, які становлять комерційну таємницю, з ціллю розголошення чи іншого незаконного використання, що можуть завдати значну шкоду суб'єкту господарювання (підприємству, установі, організації), на винних накладається покарання у вигляді штрафу від трьох до восьми тисяч неоподатковуваних мінімумів доходів громадян [7].

Згідно зі ст. 232 ККУ [7] умисні діяння щодо розголошення комерційної таємниці без наданої та те згоди власника особою, якій відома таємниця, в зв'язку зі службовою чи професійною діяльністю, на основі корисливих чи особистісних мотивів у результаті завдання шкоди суб'єкту господарювання (підприємству, організації, установі) накладається штраф у розмірі від однієї до трьох тисяч неоподаткуваних мінімумів доходів громадян, а також можливість обіймати певні посади або займатися певною діяльністю на термін до трьох років [7].

Висновки. Виходячи із ґрунтовного аналізу наукових праць [8–18], а також законодавчої та нормативно-правової бази України [1–7], слід зазначити, що від рівня захищеності інформації залежить подальший розвиток підприємства та перспектива його функціонування. Встановлено, що ключовими бізнес-індикаторами діагностики ефективності системи захисту інформації на підприємстві є: рівень цінності інформації; рівень секретності інформації; рівень доступності до інформації; рівень контролю за захистом інформації; частота і вагомість діяння щодо порушення захисту інформації. З'ясовано, що внаслідок порушення законодавства України про інформацію до винних може застосовуватись дисциплінарна, матеріальна, цивільно-правова, адміністративна та кримінальна відповідальність.

Перспективи подальших досліджень у цьому напрямі полягають у формуванні системи цілей діагностики діяльності підприємства, яка на відміну від інших містить діагностику ефективності системи захисту інформації на підприємстві з урахуванням відповідальності за порушення законодавства про комерційну таємницю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Про інформацію : Закон України від 02.10.1992 р. № 2657-XII // Відомості Верховної Ради України. – 2001. – № 12. – Ст. 64.
2. Цивільний кодекс України : Закон України від 16.01.2003 р. № 435-IV // Відомості Верховної Ради України. – 2003. – № 40–44. – Ст. 356.
3. Про перелік відомостей, що не становлять комерційної таємниці : постанова Кабінету Міністрів України від 09.08.1993 р. № 611. [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/611-93-п.
4. Господарський кодекс України : Закон України від 16.01.2003 р. № 436-IV // Відомості Верховної Ради України . – 2003. – № 18, № 19–20, № 21–22. – Ст. 144.
5. Кодекс законів про працю України : Закон України від 10.12.1971 р. № 322-VIII // Відомості Верховної Ради УРСР . – 1971. – Додаток до № 50. – Ст. 375.
6. Кодекс України про адміністративні правопорушення : Закон України від 07.12.1984 р. № 8073-X // Відомості Верховної Ради УРСР . – 1984. – Додаток до № 51. – Ст. 1122.
7. Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III // Відомості Верховної Ради України. – 2001. – № 25–26. – Ст. 131.
8. Радутний О.Е. Кримінальна відповідальність за незаконне збирання, використання та розголошення відомостей, що становлять комерційну таємницю (аналіз складів злочинів) : автореф. дис. на здобуття наук ступеня канд. юрид. наук : 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право»/ О.Е. Радутний. – Харків, 2002. – 21 с.
9. Сляднєва Г.О Право суб'єкта господарювання на комерційну таємницю та його захист: автореф. дис. на здобуття наук ступеня канд. юрид. наук : 12.00.04 «Господарське право, господарсько-процесуальне право» / Г.О. Сляднєва. – Донецьк, 2005. – 16 с.
10. Матвієнко П.Є. Адміністративна відповідальність за порушення законодавства про комерційну таємницю: автореф. дис. на здобуття наук ступеня канд. юрид. наук : 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / П.Є. Матвієнко. – Київ, 2010. – 19 с.
11. Харламова С.О. Кримінальна відповідальність за незаконні дії з відомостями, що становлять комерційну або банківську таємницю: автореф. дис. на здобуття наук ступеня канд. юрид. наук : 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право» / С.О. Харламова. – Київ, 2007. – 20 с.
12. Носік Ю.В. Права на комерційну таємницю в Україні (цивільно-правовий аспект): автореф. дис. на здобуття наук ступеня канд. юрид. наук : 12.00.03 «Цивільне право і цивільний процес; сімейне право; міжнародне приватне право» / Ю.В. Носік. – Київ, 2006. – 18 с.
13. Спільна Н.П. Методологічний підхід до оцінки економічної ефективності захисту інформації / Н.П. Спільна, Н.Д. Махновська // Экономика Крыма. – 2012. – № 3 (40). – С. 121–125.
14. Берлач А.І. Правові засади захисту комерційної таємниці в Україні / А.І. Берлач // Юридичний вісник. – 2009. – № 3 (12). – С. 37–41.
15. Килимник І.І. Правова характеристика забезпечення комерційної таємниці на підприємстві в умовах ринкової економіки : монографія / І.І. Килимник, О.В. Харитонов. – Харків: ХНУМГ, 2014. – 82 с.
16. Черевко О.В. Забезпечення режиму комерційної таємниці всередині підприємства / О.В. Черевко // Ефективна економіка. – 2013. – № 11. [Електронний ресурс]. – Режим доступу до журналу: http://www.economy.nayka.com.ua.
17. Чистоклетов Л.Г. Інформаційна безпека підприємства – як складова економічної безпеки: сучасні реалії та загрози / Л.Г. Чистоклетов // Наукові записки Львівського ун-ту бізнесу та права. – 2011. – Вип. 7. – С. 222–227.
18. Боцян Т.В. Облік і внутрішній контроль діяльності підприємств в умовах використання комп'ютерних технологій: управлінський аспект: автореф. дис. на здобуття наук ступеня канд. екон. наук : 08.06.04 «Бухгалтерський облік, аналіз та аудит» / Т.В. Боцян. – Київ, 2005. – 20 с.

УДК 342.9:341.1

ПРЕДМЕТ АДМІНІСТРАТИВНОГО ПРАВА В КОНТЕКСТІ БУДІВЕЛЬНОЇ ДІЯЛЬНОСТІ

THE SUBJECT OF ADMINISTRATIVE LAW IN CONTEXT OF CONSTRUCTION ACTIVITIES

Стукаленко О.В.,
кандидат юридичних наук, доцент кафедри адміністративного та господарського права
Одеський національний університет імені І.І. Мечникова

Стаття присвячена предмету адміністративного права в контексті будівельної діяльності. Наголошується, що наукове вирішення питань, пов'язаних із визначенням предмету адміністративного права, теоретично і практично важливе. Воно допомагає правильно осмислити ті правові процеси і явища, які відбуваються в суспільстві і державі, зрозуміти закономірності їх розвитку. Акцентується увага на групах однорідних суспільних відносин, що формуються у ході адміністративно-правового регулювання у будівельній галузі. Зазначено, що поступовий процес оновлення адміністративних правовідносин можна прослідкувати через еволюціонування поняття предмета адміністративного права.

Ключові слова: предмет адміністративного права, адміністративні правовідносини, будівельна галузь, будівельна діяльність.

Статья посвящена предмету административного права в контексте строительной деятельности. Отмечается, что научное решение вопросов, связанных с определением предмета административного права, теоретически и практически важно. Оно помогает верно осмыслить правовые процессы и явления, происходящие в обществе и государстве, понять закономерности их развития. Акцентируется внимание на группах однородных общественных отношений, которые формируются в ходе административно-правового регулирования в строительной отрасли. Указано, что постепенный процесс обновления административных правоотношений можно проследить сквозь эволюционирование понятия предмета административного права.

Ключевые слова: предмет административного права, административные правоотношения, строительная отрасль, строительная деятельность.

The article is devoted to subject of administrative law in context of construction activities. It is noted that the scientific issues related to definition of subject of administrative law theoretically and practically important. It assists to comprehend the legal processes and phenomena occurring in society and state, to understand regularities of their development. The focus is on groups of homogeneous social relations that are formed during the administrative-legal regulation in construction industry. It is indicated that the gradual process of updating administrative legal relations, can be traced through evolution of concept of subject of administrative law.

Key words: subject of administrative law, administrative legal relations, construction industry, construction activity.