1.Должанский И.З., Загорная Т.О., Удалых О.А. и др. Управление потенциалом предприятия. – Донецк-Макеевка, 2005. – 348 с.

2.Стратегічне управління потенціалом підприємства / Б.Г. Шелегеда, Н.В. Кас'янова, А.Я. Берсуцький та ін. – Донецьк: ДонУЕП, 2006. – 219 с.

3.Вейтс В. Потенциальные и кинетические производственные силы мирового хозяйства. – Кн. 1. – М., 1927. – 22 с.

4.Воблый К.Г. Производственные силы Украины. Техника, экономика и право // Научн. записки нар. хоз-ва. – 1924. – № 4-5. – С. 126-149.

5.Отенко И.П. Стратегическое управление потенциалом предприятия. – Харьков: ХНЭУ, 2006. – 256 с.

6.Акимова Т.А. Теория организации. – М.: ЮНИТИ-ДАНА, 2003. – 368 с.

7.Teece D., Pisano G., Shuen A. Dynamic Capabilities and Strategic Management. Working Paper. – Berkeley: University of Californiya at Berkeiey, 1992.

Отримано 26.03.2013

УДК 658

А.О.ЧЕРЕДНИЧЕНКО, М.Ю.КАРПУШЕНКО, канд. екон. наук
Харківська національна академія міського господарства

КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ ТА КАТЕГОРІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМІ КОРПОРАТИВНОГО УПРАВЛІННЯ БУДІВЕЛЬНИХ ПІДПРИЄМСТВ

Розглядається класифікація інформації на підприємствах з корпоративним методом управління (зокрема на підприємствах будівельної галузі). Аналізується положення нормативно-правових актів, наводиться визначення різних видів інформації з обмеженим доступом. Визначено головні категорії безпеки в системі корпоративного управління та надано пропозиції щодо поліпшення ступеню захисту такої інформації.

Рассмотрена классификация информации на предприятиях с корпоративным методом управления (в частности на предприятиях строительной отрасли). Анализируются положения нормативно-правовых актов, приводится определение различных видов информации с ограниченным доступом. Определены главные категории безопасности в системе корпоративного управления и представлены предложения по улучшению степени защиты такой информации.

The paper treats classification of information at enterprise with corporative method of management. Analyzed legal acts and given explanations of the term information with limited access. The major categories of security in corporate governance and suggestion of improvement the level of protection the information are defined in the article.

Ключові слова: інформація, безпека, класифікація інформації, категорії інформаційної безпеки.

Інформація стала першоосновою життя сучасного суспільства, предметом та продуктом його діяльності, а процеси її створення, накопичення, збереження, передачі та обробки, в свою чергу, стимулювали виробництво відповідних пристроїв, які б забезпечували таку трансформацію. У зв’язку з новими інформаційними досягненнями, державні

кордони практично стають прозорими для обігу інформації. При цьому, чим більше зазначена галузь залучається в комерційний обіг, тим більше виникає потреба в захисті інтересів власників інформації.

В період загострення конкурентної боротьби, намагань збереження позицій на будівельному ринку, отримання нових замовлень, насамперед в період світової фінансової кризи, набуває важливого значення захист ділової, фінансової, технологічної та іншої інформації від крадіжок, несанкціонованого використання, її зміни чи знищення взагалі. Успішне вирішення вказаних питань потребує комплексного, наукового, системного підходу. Дослідженням проблем захисту інформації займалися такі вчені, як Користін О.Є., Мак-Мак В., Минаєв Г.А., Судоплатов А.П. [3-6].

Термін «інформація» трактується як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Відповідно, під захистом інформації розуміється сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї [1].

Категорія «інформаційна безпека» виникла з появою засобів інформаційних комунікацій між людьми, а також з усвідомленням людиною наявності у людей і їхніх співтовариств інтересів, яким може бути завданий збитку шляхом дії на засоби інформаційних комунікацій, наявність і розвиток яких забезпечує інформаційний обмін між всіма елементами соціуму.

Суб'єкти господарювання, зацікавлені у своїй конкурентоспроможності, вживають відповідні заходи щодо захисту такої інформації, спираючись на відповідні норми чинного законодавства, норми міжнародного права та власну нормативно-правову основу [3].

Режим доступу до інформації – це передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації. За режимом доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом . Доступ до відкритої інформації забезпечується шляхом:

- систематичної публікації її в офіційних друкованих виданнях (бюлетенях, збірниках);
- поширення її засобами масової комунікації;
- безпосереднього її надання заінтересованим громадянам, державним органам та юридичним особам.

Захист інформації з обмеженим доступом є одним з першочергових завдань забезпечення інформаційної безпеки в системі корпоративного управління будівельних підприємств. Його ефективна реалізація потре-

бує чіткого розуміння понять «інформація з обмеженим доступом», «конфіденційна інформація», «комерційна інформація», «таємна інформація». Оскільки положення з цього приводу (окрім категорії «таємна») містяться переважно в актах неінформаційного характеру і є доволі суперечливими, для з'ясування суті вищезазначених термінів слід проаналізувати зміст відповідних правових норм та визначитися з категоріями інформації з обмеженим доступом, які більш притаманні саме будівельним підприємствам.

Згідно до ст. 30 Закону України "Про інформацію", інформація з обмеженим доступом за своїм правовим режимом поділяється на конфіденціальну (конфіденційну) і таємну [1].

До конфіденціальної інформації відносяться відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їхнім бажанням відповідно до передбачених ними умов [1]. Громадяни, юридичні особи, які володіють інформацією професійного, ділового, виробничого, банківського, комерційного та іншого характеру, одержаною на власні кошти, або такою, яка є предметом їх професійного, ділового, виробничого, банківського, комерційного та іншого інтересу і не порушує передбаченої законом таємниці, самостійно визначають режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлюють для неї систему (способи) захисту. Виняток становить інформація комерційного та банківського характеру, а також інформація, правовий режим якої встановлено Верховною Радою України за поданням Кабінету Міністрів України (з питань статистики, екології, банківських операцій, податків тощо), та інформація, приховування якої являє загрозу життю і здоров'ю людей.

Відповідно до ст. 36 Господарського кодексу України комерційною таємницею є відомості, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансовою та іншою діяльністю суб'єкта господарювання, розголошення яких може завдати шкоди його інтересам. З правової точки зору, комерційну таємницю часто пов’язують з засобами захисту від неякісної конкуренції в межах реалізації права на інтелектуальну власність [1]. Це положення випливає зі змісту пункту VIII статті 2 Конвенції про заснування Всесвітньої організації інтелектуальної власності, яка була підписана в Стокгольмі 14 липня 1967 року та змінена 2 жовтня 1979 року, учасником якої був колишній СРСР, а сьогодні – Україна. Неправомірне збирання, розголошення та використання комерційної таємниці є видом недобросовісної конкуренції, який може становити досить серйозну загрозу економічній безпеці фірми (підприємства). Так, за підрахунками американських фахівців, втрата 20% інформації,

що становить комерційну таємницю, веде до банкрутства фірми (організації) протягом місяця в 60 випадках із 100 [2].

До таємної належить інформація, що містить відомості, які становлять державну або іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі[1]. Інформація вказаної категорії циркулює, як правило в системі спеціальних будівельних установ, або таких які отримали закази на проектування за секретними тематиками, здійснення будівельно-монтажних, ремонтно-відновлювальних робіт на секретних об'єктах.

З погляду інформаційної безпеки для інформації можна виділити наступні категорії:

- конфіденційність – гарантія того, що конкретна інформація доступна тільки тому колу осіб, для кого вона призначена; порушення цієї категорії називається розкраданням або розкриттям інформації;
- цілісність – гарантія того, що інформація зараз існує в її початковому вигляді, тобто при її зберіганні або передачі не було проведено несанкціонованих змін; порушення цієї категорії називається фальсифікацією повідомлення;
- автентичність – гарантія того, що джерелом інформації є саме та особа, яка заявлена як її автор; порушення цієї категорії також називається фальсифікацією, але вже автора повідомлення;
- апелюємість – гарантія того, що при необхідності можна буде довести, що автором повідомлення є саме заявлена людина, і не може бути ніхто інший (часто застосовувана в електронній комерції); відмінність цієї категорії від попередньої в тому, що при підміні автора, хтось інший намагається заявити, що він автор повідомлення, а при порушенні апелюємість – сам автор намагається "відхреститися" від своїх слів, підписаних ним одного разу.

У відношенні інформаційних систем слід застосовувати наступні категорії:

- надійність – гарантія того, що система поводиться в нормальному і позаштатного режимах так, як заплановано;
- точність – гарантія точного і повного виконання всіх команд;
- контроль доступу – гарантія того, що різні групи осіб мають різний доступ до інформаційних об'єктів, і ці обмеження доступу постійно виконуються;
- контрольованість – гарантія того, що в будь-який момент може бути проведена повноцінна перевірка будь-якого компонента програмного комплексу;
- контроль ідентифікації – гарантія того, що клієнт, підключений у даний момент до системи, є саме тим, за кого себе видає;

❖ стійкість до умисних збоїв – гарантія того, що при умисному внесенні помилок у межах заздалегідь обговорених норм система буде вести себе так, як обумовлено заздалегідь [3].

Таким чином, з урахуванням визначених категорій інформаційна безпека організації це цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток.

Для реалізації захищеності інформаційного середовища організації підприємства чи установи необхідно функціонування саме комплексної системи захисту, яка включатиме механізми фізичної охорони, технічний, інтелектуальний, правовий захист відомостей, матеріальних носіїв,об'єктів підприємств та установ тощо. Але ж у сучасних умовах в будівельній галузі України така цілісна система щодо комплексного захисту інформаційного середовища фактично не функціонує з ряду об'єктивних та суб'єктивних причин, до яких слід віднести ліквідацію потужних державних будівельних спеціалізованих підприємств, де вона діяла, втрата кадрового потенціалу, фахівців з охорони й захисту, зміни в законодавчо-нормативній базі, політики оптимізації та скорочення непрофільних напрямків діяльності тощо. Для реалізації захищеності інформаційного середовища організації підприємства чи установи в системі корпоративного управління будівельними підприємствами необхідно створити або відновити окремі самостійні підрозділи з захисту інформаційних ресурсів, які будуть проводити аналітичну роботу, надавати керівництву установи прогнози і пропозиції щодо підвищення рівня захисту інсайдерської інформації.

1. Про інформацію: Закон України від 02.10.1992 р. // Закони України. – К., 1996. – Т.4.

2. Про перелік відомостей, що не становлять комерційної таємниці: постанова Кабінету Міністрів України від 9 серпня 1993 р. № 611 // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua.

3. Економічна безпека / Користін О.Є., Барановський О.І., Герасименко Л.В., Доля Л.М., Калюк О.М. та ін. – К.: Всеукраїнська асоціація видавців "Правова єдність"; Алерта; КНТ; Центр учбової літератури, 2010. – 368 с.

4. Мак-Мак В. Служба безопасности предприятия. Организационно-управленческие и правовые аспекты деятельности / В. Мак-Мак. – М.: Мир безопасности, 2000. – 189 с.

5. Минаев Г.А., Теория безопасности организации / Г.А. Минаев, А.А. Прохожев. – М.: РАГС, 2004. – 165 с.

6. Судоплатов А.П. Безопасность предпринимательской деятельности / А.П. Судоплатов, С.В. Лекарев. – М.: ОЛМА-ПРЕСС, 2001. – 382 с.

Отримано 26.02.2013