

УДК 624:658.5.003.1

УПРАВЛІННЯ ПЕРСОНАЛОМ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БУДІВЕЛЬНИХ ПІДПРИЄМСТВ

аспірант, Чередниченко А. О.

Харківський національний університет міського господарства

ім. О. М. Бекетова, Україна, м Харків

Визначено, що вагомим джерелом інформаційних загроз будівельного підприємства є його персонал, ефективне управління яким дозволяє забезпечити прийнятний рівень інформаційної безпеки. Розкрито заходи щодо управління персоналом в системі забезпечення інформаційної безпеки. Запропоновано підхід до оцінки надійності управлінського персоналу за інтегральними показниками наступних компонент: інформаційно-професійної компетентності, лояльності, комунікабельності. Бальна оцінка показників проводиться експертами з урахуванням пріоритетності показників, котра визначається методом аналізу ієрархій. Отримані результати оцінювання дозволяють більш обґрунтовано обрати заходи щодо забезпечення інформаційної надійності.

Ключові слова: управління персоналом, інформаційна безпека, оцінка надійності, будівельні підприємства.

Чередниченко А. А. Управление персоналом в контексте обеспечения информационной безопасности строительных предприятий/ Харьковский национальный университет городского хозяйства им. О. Н. Бекетова, Украина, г. Харьков.

Определено, что весомым источником информационных угроз строительного предприятия является его персонал, эффективное управление которым позволяет обеспечить приемлемый уровень информационной безопасности. Раскрыты мероприятия по управлению персоналом в системе

обеспечения информационной безопасности. Предложен подход к оценке надежности управленческого персонала по интегральным показателям следующих компонент: информационно-профессиональной компетентности, лояльности, коммуникабельности. Бальная оценка показателей проводится экспертами с учетом приоритетности показателей, которая определяется методом анализа иерархий. Полученные результаты оценивания позволяют более обосновано выбрать мероприятия по обеспечению информационной надежности.

Ключевые слова: управление персоналом, информационная безопасность, оценка надежности, строительные предприятия.

Cherednichenko A. O. Management of the personnel in the context of ensuring the information security of the building enterprises /O. M. Beketov National University of Urban Economy in Kharkiv, Ukraine, Kharkiv.

Determined that a significant source of information threats of building enterprise is its personnel), the effective management of which enables to ensure an acceptable level of information security. Are disclosed events on management personnel in information security system. Proposed an approach to assessing the reliability of administrative staff at Integral Indicators of the following components: information and professional competence, loyalty, sociability. Point scoring indicators conducted by experts, taking into account the priority indicators, which is determined by the method of analysis of hierarchies. The results of the evaluation allow to choose measures to ensure information reliability.

Keywords: management of the personnel, informative safety, reliability estimation, building enterprises.

Вступ

Практична реалізація положень сформованої політики інформаційної безпеки будівельних підприємств потребує дієвих практичних зусиль із забезпечення управління персоналом з урахуванням вимог забезпечення інформаційної безпеки. Персонал підприємства часто є основним суб'єктом

реалізації загроз інформаційної безпеки. Безвідповідальність персоналу виявляється в порушенні співробітниками діючих на підприємстві вимог із забезпечення інформаційної безпеки, що приводить до витоку конфіденційних відомостей в самих різних формах і вимагає відповідного інформаційній безпеці управління персоналом.

Питання інформаційної безпеки та управління персоналом в напрямку її забезпечення вивчаються в працях таких вчених в даній галузі як В. В. Андріанов, С. Л. Зефіров, В. Б. Голованов, Н. А. Голдуєв, А. А. Анісімов, О. В. Герасименко, А. В. Козак, М. І. Глухов, О. О. Кузнецов, С. П. Євсєєв, С. В. Кавун та інші [1-5].

Однак вирішення проблем забезпечення інформаційної безпеки потребують подальшого вивчення й удосконалення заходів ефективного управління персоналом в контексті протидії інформаційним загрозам.

Метою статті є обґрунтування складових управління персоналом та методики оцінки надійності персоналу в контексті забезпечення інформаційної безпеки будівельних підприємств.

Одним з основних і найскладніших напрямів системи управління інформаційною безпекою є робота з персоналом, мета якої:

- відбір і попередня перевірка персоналу, що приймається на роботу;
- навчання та мотивація співробітників в аспекті інформаційної безпеки;
- досягнення взаєморозуміння керівників і співробітників в питаннях забезпечення інформаційної безпеки;
- контроль за дотриманням працівниками режиму забезпечення інформаційної безпеки.

В системі забезпечення інформаційної безпеки будівельних підприємств необхідно реалізовувати дієві заходи з протидії виникнення інформаційних загроз щодо персоналу, який має справу з конфіденційною інформацією підприємства.

Так, при прийомі на роботу рекомендується проводити анкетування, за

допомогою якого можна зробити висновки про рівень інтелекту, отримати загальне уявлення про кандидата як різносторонньої особи, визначити морально-психологічний рівень, виявити можливі злочинні схильності і т.д.

У разі успішного проходження кандидатом перевірки і визнання його відповідним посаді здійснюється підписання двох документів:

а) трудового договору (контракту). Контракт обов'язково повинен містити пункт про обов'язок працівника не розголошувати конфіденційну інформацію і дотримувати заходи безпеки;

б) договору (зобов'язання) про не розголошування конфіденційної інформації, є правовим документом, в якому кандидат на вакантну посаду дає обіцянку не розголошувати ті відомості, які йому буде відомий в період його роботи на підприємстві, а також про відповідальність за їх розголошування або недотримання правил безпеки (розірвання контракту і судовий розгляд).

Велику значимість в загальній системі заходів з подолання впливу людського чинника має повсякденна робота з персоналом. Організація персоналу включає навчання співробітників правилам і прийомам роботи з конфіденційною інформацією. Навчання може бути диференційовано залежно від терміну роботи співробітників на підприємстві - тобто програма навчання для нових співробітників і для співробітників, які мають досвід роботи в даній організації. Крім навчання персоналу, однією з основних задач є постійне нагадування всім співробітникам про необхідність дотримання правил інформаційної безпеки.

Мотивація співробітників підприємства в цілях забезпечення його інформаційної безпеки може реалізовуватися по двох напрямках - шляхом застосування заохочень і санкцій.

Невід'ємним елементом управління персоналом є контроль за дотриманням співробітниками правил забезпечення інформаційної безпеки і за надійністю персоналу.

Контроль дотримання правил забезпечення безпеки може проводитися з використанням: планових і раптових перевірок, в процесі яких служба

безпеки перевіряє дотримання в структурних підрозділах правил роботи з конфіденційною інформацією, а також працездатність технічних засобів захисту; моніторингу ситуації силами позаштатних інформаторів служби безпеки з числа співробітників відповідних підрозділів; моніторингу ситуації з використанням спеціальних технічних засобів спостереження.

Контроль надійності персоналу здійснюється службою безпеки в індивідуальному режимі відносно окремих категорій співробітників. В першу чергу, це менеджери, експерти і рядові виконавці, що займають ключові робочі місця, що забезпечують доступ до конфіденційної інформації. Контроль їх лояльності здійснюється в постійному режимі [6].

Для підвищення загальної ефективності необхідно проводити оцінку надійності даного персоналу. Аналіз підходів до оцінки надійності персоналу показав, що основною характеристикою надійності є лояльність персоналу до підприємства [1, 6, 7]. Вважаємо, що в системі інформаційної безпеки будівельних підприємств рівень надійності також повинні визначати інформаційна і професійна компетентність, а також рівень комунікабельності як здатність до ефективної взаємодії.

Виходячи з зазначеного вдосконалений підхід до оцінки надійності персоналу як елемента забезпечення інформаційної безпеки через формування комплексного показника, що включає характеристики надійності по трьох напрямках: інформаційно-професійна компетентність, лояльність, комунікабельність. Загальна схема методики оцінки надійності управлінського персоналу представлена на рис. 1.

З метою оцінювання розроблені анкети, в яких експерти мають оцінити інформаційну надійність обраного співробітника. На основі експертних оцінок формуються інтегральні оцінки за компонентами, лояльність, комунікабельність. Пріоритетність компонент та показників визначають експерти шляхом застосування способу аналізу ієрархій з використанням шкали Сааті.

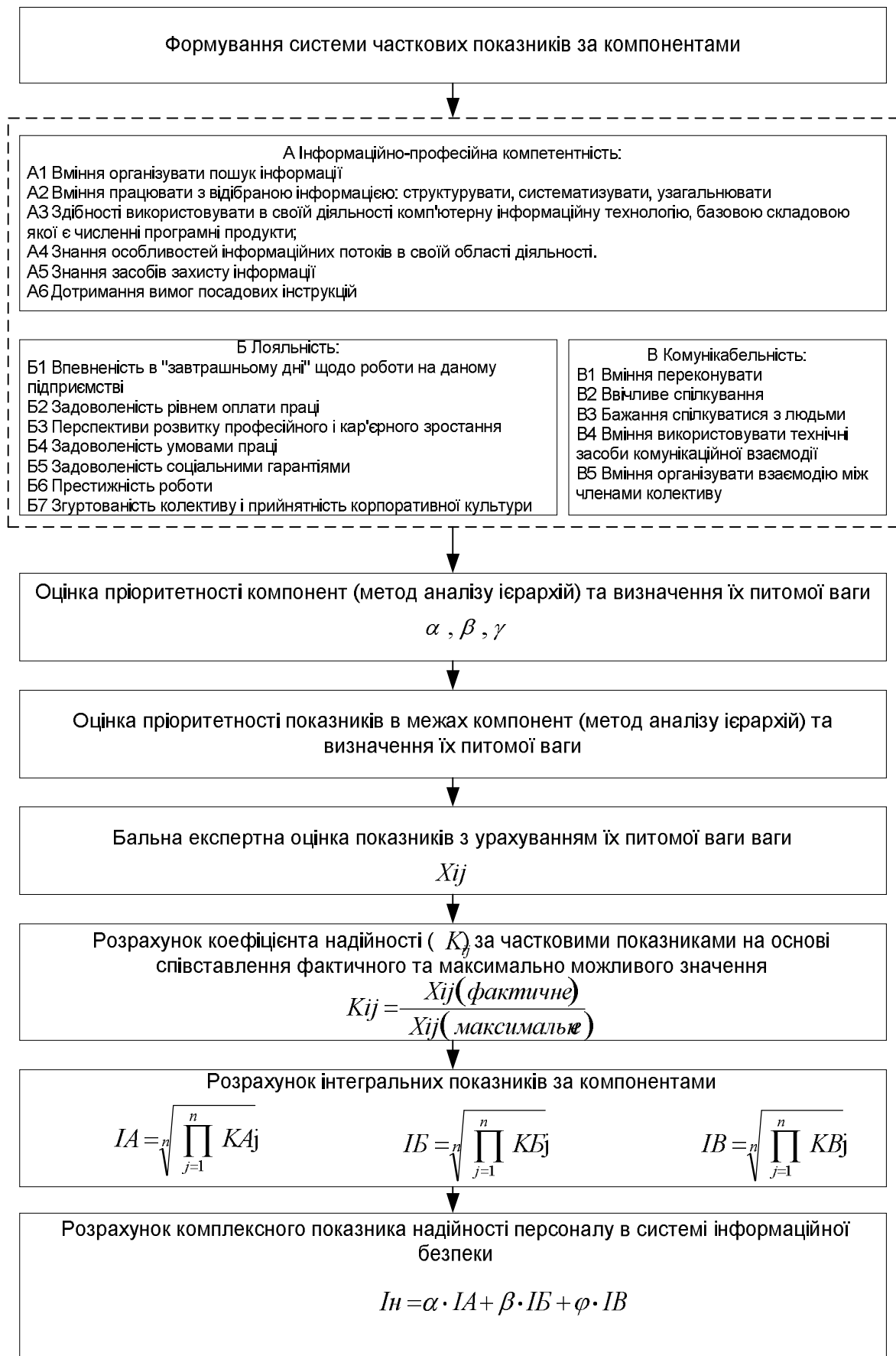


Рис. 1. Алгоритм оцінки надійності управлінського персоналу в системі інформаційної безпеки

За методикою, що пропонується проведена оцінка надійності менеджера будівельного підприємства. Отримані значення показників надійності відображено на рис. 2.

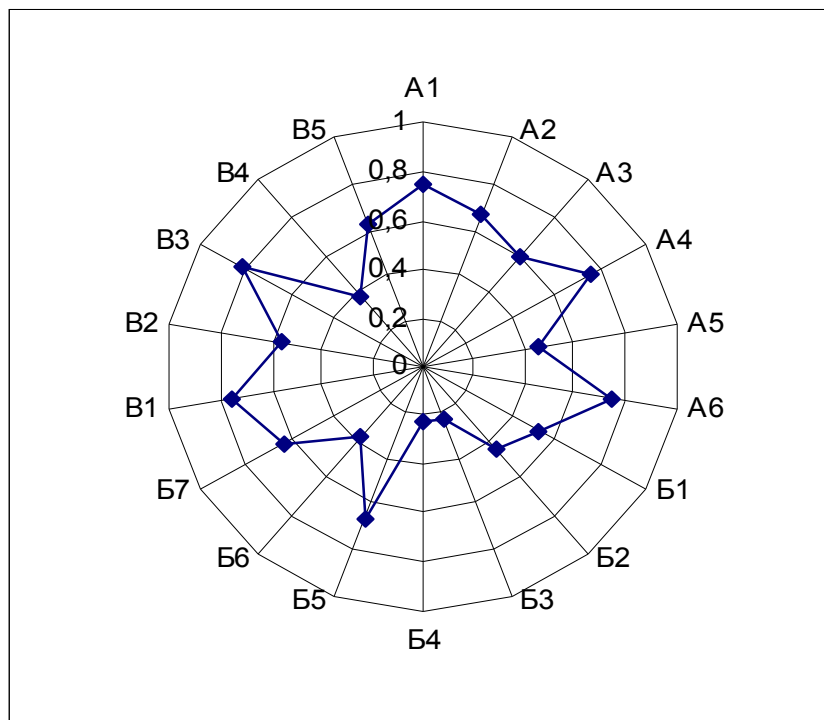


Рис.2. Результати експертної оцінки показників, що характеризують надійність працівника в системі інформаційної безпеки

Розраховано інтегральні показники за компонентами (А інформаційно-професійна компетентність, Б лояльність та В комунікабельність).

$$K_A = \sqrt[6]{0,74 \cdot 0,66 \cdot 0,58 \cdot 0,76 \cdot 0,46 \cdot 0,74} = 0,65$$

$$K_B = \sqrt[7]{0,52 \cdot 0,4 \cdot 0,22 \cdot 0,24 \cdot 0,66 \cdot 0,38 \cdot 0,62} = 0,4$$

$$K_V = \sqrt[5]{0,75 \cdot 0,56 \cdot 0,82 \cdot 0,38 \cdot 0,62} = 0,6$$

Визначено комплексний показник надійності працівника в системі інформаційної безпеки

$$K_H = 0,26 \cdot 0,65 + 0,57 \cdot 0,4 + 0,17 \cdot 0,6 = 0,55$$

Отриманий результат, що встановлює кількісний вимір рівня надійності може бути інтерпретованим в такій шкалі оцінювання:

$0 < K_n < 0,33$ - рівень надійності критичний, відрізняється незадоволеність роботою на підприємстві, низькою компетентністю, що створює умови для виникнення загроз інформаційної безпеки;

$0,34 < K_n < 0,66$ – рівень ймовірністний - низька зацікавленість в роботі на даному підприємстві, працівник безініціативний щодо діяльності із забезпечення інформаційної безпеки;

$0,67 < K_n < 1$ – задовільний рівень надійності характеризується тим, що працівник лояльний, націлений на подальшу роботу на даному підприємстві, своїми діями спроможний протидіяти загрозам інформаційної безпеки.

Визначений рівень надійності характеризується як ймовірністний, що свідчить про вірогідність виникнення загроз інформаційної безпеки від працівника. Зокрема, спостерігаємо найнижчий рівень таких характеристик, як перспективи розвитку професійного і кар'єрного зростання, задоволеність умовами праці, престижність роботи та вміння використовувати технічні засоби комунікаційної взаємодії.

Висновки

Таким чином, комплекс всіх організаційних заходів по роботі з персоналом будівельного підприємства, що включає систему планування, навчання персоналу, систему залучення порушників до відповідальності, і постійну підтримку атмосфери відповідального відношення до питань безпеки, повинен до певної міри зменшити негативний вплив людського чинника на захищеність інформаційних систем і стан інформаційної безпеки. Важливим напрямком роботи в системі управління кадрами в контексті забезпечення інформаційної безпеки є оцінка надійності працівників. Використання запропонованої методики для оцінки надійності управлінського персоналу дозволяє обрати відповідні ситуації заходи щодо протидії виникнення й реалізації інформаційних загроз.

Література:

1. Андрианов В. В. Обеспечение информационной безопасности бизнеса [Электронный ресурс] / В. В. Андрианов, С. Л. Зефирова, В. Б. Голованов, Н. А. Голдусев. – Режим доступа:
http://bezopasnik.org/article/book/andrianov_infobez_biz_2011.pdf
2. Анисимов А. А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А. А. Анисимов. - Режим доступа:
http://www.intuit.ru/goods_store/ebooks/8468
3. Герасименко О. В. Інформаційна безпека підприємства: поняття та методи її забезпечення / О. В. Герасименко, А. В. Козак [Електронний ресурс]. – Режим доступу:
<http://intkonf.org/kengerasimenkoovkozakavinformatsiynabezpekapidpriemstvaonyattayatametodiyiyizabezpechennya>
4. Глухов Н. И. Информационная безопасность предприятия / Н. И. Глухов. - Иркутск: РИО СИПЭУ, 2008. -194 с.
5. Кузнецов О. О. Захист інформації та економічна безпека підприємства: монографія / О. О. Кузнецов, С. П. Євсєєв, С. В. Кавун. - Харків: Вид. ХНЕУ, 2008. - 360 с.
6. Алавердов А. Р. Управление кадровой безопасностью организации/ А. Р. Алавердов. - М.: Маркет ДС, 2008. 176 с.
7. Управление персоналом: учебник / [Е. Л. Аксенова, Т. Ю. Базаров, Б. Л. Еремин]; под ред. Т. Ю. Базарова. – [2-е изд., перераб. и доп.]. – М: Юнити-Дана, 2002. – 560 с.

References:

1. Andryanov V. V. Obespechenye ynformatsyonnoy bezopasnosty byznesa [Web Resource] / V. V. Andryanov, S. L. Zefyrov, V. B. Holovanov, N. A. Holduev. – URL:
http://bezopasnik.org/article/book/andrianov_infobez_biz_2011.pdf
2. Anysymov A. A. Menedzhment v sfere ynformatsyonnoy bezopasnosty [Web Resource] / A. A. Anysymov.- URL: [://www.intuit.ru/goods_store/ebooks/8468](http://www.intuit.ru/goods_store/ebooks/8468)
3. Herasimenko O. V., Kozak A. V. Informatsiina besheka pidpriemstva: poniattia ta metody ii zabezpechennia [Web Resource] / O. V. Herasimenko, A. V. Kozak/ - URL: <http://intkonf.org/kengerasimenkoovkozakavinformatsiynabezpekapidpriemstvaonyattyatametodiyiyizabezpechennya>

4. *Hlukhov N. Y. Ynformatsyonnaya bezopasnost' predpryyatyia / N. Y. Hlukhov. - Yrkut-sk: RYO SYPЭU, 2008. -194 p.*
5. *Kuznetsov O. O. Zakhyst informatsii ta ekonomichna pezpeka pidpryiemstva: monohrafiia / O. O. Kuznetsov, S. P. Ievseev, S. V. Kavun. - Kharkiv, KhNEU, 2008, 360 p.*
6. *Alaverdov A. R. Upravlenye kadrovoy bezopasnost'yu orhanyzatsyy /A. R. Alaverdov. - M.: Market DS, 2008. 176 p.*
7. *Upravlenye personalom: uchebnyk / [E. L. Aksenova, T. Yu. Bazarov, B. L. Eremyn]; pod red. T. Yu. Bazarova. – [2-e yzd., pererab. y dop.]. – M: Yunyty-Dana, 2002. – 560 p.*