

## ОРГАНІЗАЦІЯ РОБОТИ ПІДРОЗДІЛУ ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

### Вступ

Роль інформації з обмеженим доступом в підприємницькій діяльності набуває все більшого значення, тому організація забезпечення безпеки бізнеса є актуальною проблемою і пов'язана із розв'язком задач захисту та автоматизованою обробкою інформації з обмеженим доступом. Кожне підприємство, установа, організація, яка приймає необхідні дії збереження інформації від витоку, застосування прогресивних технічних засобів призначених для роботи з матеріальними носіями інформації підвищує рівень безпеки, а відповідно і рівень довіри до свого підприємства, установи, організації у середовищі клієнтів та партнерів. Тому питання конфіденційності, цілосності і доступності інформації з обмеженим доступом та її автоматизація обумовлюють конкретизацію задач безпеки, які необхідно вирішити на підприємстві в організації і установі. На сьогодні можна стверджувати, що відсутність єдиної методології у вирішенні цих питань у сукупності до певної міри затримує ефективне впровадження необхідних заходів, не дає можливості керівникам проводити відповідну технічно-інформаційну політику.

Витрати на створення та експлуатацію системи безпеки інформаційної з обмеженим доступом та її автоматизації повинні бути економічно обґрунтованими [1]. Часто відсутність знань в спеціальній області призводить до значних витрат (екранування приміщень, використання дорогої техніки замість більш дешевої, но достатньо ефективної, боротьба із неіснуючими загрозами тощо), які не впливають на загальний рівень захисту та атоматизації обробки інформації.

В даній статті зупинимось більш детально на аспекті нормування праці працівникам підрозділу захисту інформації з обмеженим доступом, організація робочого місця працівників, обґрунтування вибору типів і кількості технічних засобів призначених для роботи з матеріальними носіями інформації з обмеженим доступом та рівені використання технічних засобів.

### Актуальні проблеми

До інформації з обмеженим доступом підприємства, установи, організації відносяться інформація пов'язана з науково-дослідними, дослідно-конструкторськими та дослідно-технологічними роботами а також фінансовою, технологічною та іншою інформацією яка не складає державну таємницю та конфіденційну інформацію, що є власністю держави, розголошення якої може завдати шкоди життєво важливим інтересам підприємству, установі організації. Під розголошенням інформації з обмеженим доступом розуміються протиправні, умисні або необережні дії осіб, що привели до предчасного розголошення, не викликаного службовою необхідністю, у вигляді відкритого опублікування, а також передача інформації іншим підприємствам, установам, організаціям, фізичним особам, по відкритим технічним каналам або робота з неї на некатегоровоному обладнанні.

Відповідальність за забезпечення режиму при роботі з матеріальними носіями інформації з обмеженим доступом, своєчасну розробку і здійснення необхідних заходів по її збереженню покладається на керівника підприємства, установи, організації, його заступників по напрямках і керівників структурних підрозділів. Відповідальність за організацію і здійснення робіт по захисту інформації з обмеженим доступом і проведення постійного контролю за її дотриманням покладається на підрозділ захисту інформації з обмеженим доступом або спеціально призначеним наказом керівника працівник.

Захист інформації з обмеженим доступом передбачає:

– порядок визначення інформації, яка становить інформації з обмеженим доступом і строк її дії;

- систему допуску та доступу працівників підприємства, установи, організації, відряджених і приватних осіб до матеріальних носіїв інформації з обмеженим доступом;
- порядок роботи з матеріальними носіями інформації з обмеженим доступом;
- забезпечення зберігання документів, справ і інших матеріальних носіїв інформації з обмеженим доступом та їх знищення;
- обов'язки працівників допущених до матеріальних носіїв інформації з обмеженим доступом;
- принципи організації і проведення контролю за забезпеченням режиму при роботі з матеріальних носіїв інформації з обмеженим доступом;
- відповідальність за розголошенням відомостей, втрату документів які містять інформації з обмеженим доступом.

#### **Нормування праці працівникам підрозділу захисту інформації з обмеженим доступом**

Мета нормування праці складається в тому, щоб визначити чисельність працівників необхідних для ефективного виконання всього обсягу робіт підрозділом захисту інформації з обмеженим доступом на підприємстві в установі, організації, встановити трудоміскість виконання окремих робіт, а також для вірного визначення кількості виконавців, врахувати індивідуальний вклад кожного з них в загальну працю [2].

Розподіл загальної нормативної чисельності працівників підрозділу захисту інформації з обмеженим доступом по дільницям роботи (функціям) проводиться на основі знань норм часу (виробітку), норм обслуговування, нормативів чисельності підрозділу, а в разі їх відсутності – шляхом хронометражних вимірів.

Норми часу на окремі роботи розраховуються по формулі:

$$Ч = Ч_0 (1 + \sum C/100), \quad (1)$$

де  $Ч_0$  – оперативний час, який є сумою основного та допоміжного часу, необхідного для виконання одиниці обсягу конкретної роботи;

$\sum C$  – сума часу на підготовчо- заключні роботи, організацію обслуговування робочого місця, відпочинок та особисті потреби, проценти до оперативного часу (середнє значення  $C = 8\%$ ).

На основі норм часу визначається трудоміскість окремих видів робіт (операцій). При цьому чисельність працівників підрозділом захисту інформації з обмеженим доступом ( $П$ ) визначається шляхом розділу сумарної трудоміскості робіт – нормованих ( $T_n$ ) і ненормованих ( $T_{ne}$ ) – на фонд робочого часу одного працівника ( $\Phi_{рч}$ ):

$$П = (T_n + T_{ne}) / \Phi_{рч}, \quad (2)$$

Нормативна тривалість робочого часу працівника не може перевищувати 40 годин на тиждень.

При введенні та використанні типових норм часу бажано провести організаційно-технічні засоби по створенню відповідних умов праці виконавцям (організація робочого місця, оснащення оргтехнікою тощо) та провести їх інструктаж.

#### **Організація робочого місця**

При плануванні приміщення для роботи підрозділом захисту інформації з обмеженим доступом необхідно врахувати наступне:

- столи розміщуються перпендикулярно вікну, щоб світло падало зліва (недопустимо, щоб вікно розміщувалося за спиною працівника);
- столи співробітників, які під час роботи контактують друг з другом розміщуються поряд;
- ширина проходу між столами і обладнанням для одного співробітника – 50...55 см, для двох – 65...75 см, для трьох – 95...100 см;
- відстань від робочого місця до стіни – не більше 120 см, до шафи (стілажа) – не більше 160 см;
- робочі місця співробітників, котрі повинні відвідувати інші підрозділи або контактувати з співробітниками інших служб, розміщуються неподалік від входу до приміщення.

Одної з основних предпосилок раціональної роботи підрозділу є обґрунтований вибір типів і кількості технічних засобів призначених для роботи з матеріальними носіями інформації з обмеженим доступом. Вони можуть бути визначені по наступній схемі:

– на основі технології роботи з матеріальними носіями інформації з обмеженим доступом встановлюється перелік конкретних задач і видів робіт, котрі повинні виконуватися за допомогою атестованих технічних засобів;

– визначаються типи атестованого обладнання яке доцільно застосувати для вирішення поставлених задач і намічає організаційні форми їх використання (централізовано або децентралізовано);

– встановлює обсяг робіт конкретних атестованих технічних засобів на протязі місяця або року;

– на основі підрахунку економічної ефективності уточнює типи атестованих технічних засобів, котрі повинні використовуватися, та визначає їх кількість.

Кількість одиниць атестованого обладнання необхідного для визначеної групи робіт, встановлюється по формулі:

$$H = O_i / P_{\phi} K_{zm} K_n P_n, \quad (3)$$

де  $O_i$  – обсяг інформації, котра повинна опрацьовуватися на атестованому обладнанні, натуральних одиницях (аркушах, кресленнях, одиницях виміру тощо);

$P_{\phi}$  – плановий фонд робочого часу на розрахунковий період, місяць, рік;

$K_{zm}, K_n$  – відповідно коефіцієнт змінності і планового часу роботи атестованого обладнання;

$P_n$  – планова норма напрацювання одиниці атестованого обладнання даного типу з урахуванням підготовчого та заключного часу.

#### **Рівень використання технічних засобів**

З метою вдосконалення атестованих технічних засобів необхідна кількісна оцінка досягнутого і проектного рівня автоматизації і механізації, а також технічного оснащення.

Рівень автоматизації і амеханізації визначається по формулі:

$$A = T_a / T_a + T_p, \quad (4)$$

де  $T_a, T_p$  – відповідно трудоміскість робіт, виконаних автоматизованим (механізованими) засобами і вручну за даний період, нормо-годин.

Коефіцієнт технічного оснащення розраховується по формулі:

$$K_{to} = B / CH, \quad (5)$$

де  $B$  – балансова (фактична) вартість засобів автоматизації (механізації), яка мається в підрозділі, тис. грн.;

$Ч$  – середньосписочна чисельність персоналу, чол.;

$H$  – оснащеність засобами автоматизації (механізації) в середньому на одного працівника підрозділу, грн./працівника.

Рівень технічного оснащення характеризує середній рівень оснащення одного працівника підрозділу засобами автоматизації і механізації:

$$P = B / Ч, \quad (6)$$

де  $B$  – балансова (фактична) вартість засобів автоматизації (механізації), яка мається в підрозділі, тис. грн.;

$Ч$  – середньосписочна чисельність персоналу підрозділа, чол.;

Коефіцієнт використання засобів механізації характеризується ступінню використання технічних засобів та визначається за формулою:

$$K_{em} = \Phi_f / \Phi_n, \quad (7)$$

де  $\Phi_f$ ,  $\Phi_n$  – відповідно фактичний сумарний та нормативний (розрахунковий) час використання технічних засобів механізації в даний період.

Коефіцієнт оснащення засобами механізації і використання цих засобів є інтегральним показником для оцінки механізації

$$K = K_{to} / K_{em}, \quad (8)$$

де  $K_{to}$  – коефіцієнт технічного оснащення;

$K_{em}$  – коефіцієнт використання засобів механізації.

Засоби механізації використовуються як централізовано, так і децентралізовано. Вибір організаційних форм використання засобів визначається з врахуванням вимог їх раціональної завантаженості, технічних можливостей та умов експлуатації. Основна частина технічних засобів використовується централізовано.

### Висновки

Викладені загальні підходи з використанням результатів опублікованих праць, нормативних матеріалів, сучасних стандартів до нормування праці працівникам підрозділу захисту інформації з обмеженим доступом, організація робочого місця працівників, обґрунтування вибору типів і кількості технічних засобів призначених для роботи з матеріальними носіями інформації з обмеженим доступом та рівені використання технічних засобів.

### Список літератури

1. Габович А.Г., Головань С.М., Жлобін С.І., Хорошко В.О. За ред. проф. В.О.Хорошка. Конфіденційний документообіг – К.: ДУІКТ, 2005. – 264 с.
2. Давиденко А.М., Головань С.М., Щербина В.П. Вибір оптимального складу підрозділу захисту інформації з обмеженим доступом // Моделювання та інформаційні технології. Збірник наукових праць ІПМЕ НАН України. Вип 25 – К.: – 2003, С. 67-72.

УДК 338.47

Н.Я. Кривицкая, Л.Н.Скачек,  
А.В.Титов, В.А.Хорошко

### КЛАССИФИКАЦИЯ СОВРЕМЕННЫХ ЭКОНОМИЧЕСКИХ РИСКОВ

В последние годы в связи со становлением рыночной экономики в Украине отечественные ученые стали уделять большое внимание экономическому риску. Появилось много работ в этом направлении, в том числе и работы: Альгина А.П., Балабанова И.Т., Клейнера Г.Б., Шапира В.Д. и др.

В последнее время сложилось несколько видов трактовки понятия экономического риска. Наиболее часто используется определение – вероятность опасности или деятельность, которая приводит к ущербу. Эти расхождения связаны с особенностями областей применения категории «риск» - экономической, юридической, политической, социологической и др.

С учетом толкования в общепонятийном смысле, необходимости экономического анализа и математической оценки его существенности для объекта анализа (носителя риска) представляется целесообразным определение экономического риска как вероятность потерь, возникающих при принятии и реализации экономических решений.