УДК 65.012.8

ПІДВИЩЕННЯ РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗА ДОПОМОГОЮ ОРГАНІЗАЦІЙНИХ ЗАХОДІВ НА КОМЕРЦІЙНИХ ПІДПРИЄМСТВАХ

Бурцева Катерина Анатоліївна,Тимофєєв Дмитро Сергійович
Державний ВНЗ «Національний гірничий університет», www.nmu.org.ua, elvierace@rambler.ru

Розглядаються організаційні принципи, умови та запропоновано можливі заходи з підвищення рівня інформаційної безпеки комерційного підприємства, а також організаційні методи захисту інформації як один із механізмів управління інформаційною безпекою.

Ключові слова – інформаційна безпека підприємства, організаційний захист інформації на підприємстві, організаційні методи, умови, принципи та заходи, захист інформації, система мір по захисту інформації.

ВСТУП

Інформаційна безпека підприємства ─ це захист інформації, якою володіє підприємство (виробляє, передає або отримує) від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок при надходженні. Крім того, під інформаційною безпекою розуміють захищеність інформації та підтримуючої її інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може з'явитися нанесення збитку самої інформації, її власникам або підтримуючої інфраструктури. [3]

Система мір по захисту інформації в широкому розумінні повинна бути основана виходячи із початкових умов і факторів,котрі, в свою чергу, визначаються станом спрямованості розвідок противника або діями конкурента на ринку товарів та послуг, які направлені на захоплення інформації, яка повинна бути захищена.[4]

Сучасні умови конкуренції та ведення підприємницької діяльності в країні потребують комплексного підходу до зберігання комерційної таємниці, основою якої є організаційні заходи.

ОРГАНІЗАЦІЙНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Організаційний захист інформації на підприємстві – регламентація виробничої діяльності і взаємовідношень суб'єктів (співробітників підприємства) на нормативно-правовій основі, яка ослаблює чи виключає нанесення збитків[5].

Організаційний захист інформації включає в себе наступні компоненти:

- Організація роботи з персоналом;
- Організація внутрішньооб'єктового і пропускного режимів і охорони;
- Організація роботи з носіями відомостей, що відносятся до комерційної таємниці;
- Комплексне планування заходів щодо захисту інформації;
- Організація аналітичної роботи і контроля роботи на даному підприємстві

Основні принципи організаційного захисту інформації:

- принцип комплексного підходу — ефективне використання сил, засобів, способів і методів захисту інформації для вирішення поставлених завдань залежно від конкретної ситуації, що складається, і наявності чинників, що ослабляють або підсилюють загрозу інформації, що захищається;
- принцип оперативності ухвалення управлінських рішень (істотно впливає на ефективність функціонування і гнучкість системи захисту інформації і відображає націленість керівництва і персонала підприємства на вирішення задач захисту інформації);
- принцип персональної відповідальності – найбільш ефективний розподіл задач з захисту інформації між керівництвом і персоналом підприємства і визначення відповідальності за повноту та якість їх виконання.

Серед основних умов організаціного захисту інформації можно відділити наступне:

- неперервність всебічного аналізу функціонування системи захисту інформації з метою прийняття своєчасних мір з підвищення її ефективності;
- повне дотримання керівництвом і персоналом підприємства установлених норм та правил захисту інформації.

Передача інформації, в установленому порядку, віднесеної до комерційної таємниці чи той, що містить в собі персональні данні співробітника, повинна здійснуватися на основі договора, що передбачує взаємні зобов'язання сторін по нерозголошенні цієї інформації, а також необхідні міри з її захисту.[2]

Організаційні механізми захисту інформації визначають порядок і умови комплексного використання наявних сил і засобів, ефективність якого залежить від вживаних методів технічного і економічного характеру.

Організаційні заходи захисту можуть бути або включати в себе наступне:

1. Встановлення персональної відповідальності за забезпеченням захисту інформації.
2. Обмеження доступу в приміщення, де проходить підготовка і обробка інформації.
3. Доступ до обробки, збереження і передачі конфіденційної інформації тільки перевіреним посадовим особам.

4. Призначення конкретних зразків технічних засобів для обробки цінної інформації і подальша робота тільки на них.

5. Збереження магнітних носіїв, жорстких копій і реєстраційних матеріалів в закритих міцних шафах (бажано в сейфах).

6. Виключення перегляду сторонніми особами змісту оброблюваної інформації за рахунок невідповідного встановлення дисплея, клавіатури, принтера і т.д.

7. Постійний контроль пристроїв виводу цінної інформації на фізичні носії.

8. Збереження цінної інформації на зовнішніх носіях тільки в засекреченому вигляді.

9. Використання криптографічного закриття при передачі по каналах зв'язку цінної інформації.

10. Знищення фізичних носіїв або матеріалів, що можуть містити фрагменти цінної інформації.

11. Заборона ведення переговорів про безпосередній зміст цінної інформації особам, які зайняті її обробкою.

12. Чітка організація робіт і контроль виконання.[1]

ВИСНОВОК

Приведений перелік організаційних методів не є вичерпним і, залежно від специфіки діяльності підприємства, міри конфіденційності використовуваної інформації, об'єму виконуваних робіт, а також досвіду роботи в області захисту інформації, може бути доповнений іншими методами.

ПЕРЕЛІК ВИКОРАСТАНИХ ДЖЕРЕЛ

1. Садердинов А. А., Трайнев В. А., Федулов А. А. Информационная безопасность предприятия: Учебное пособие.2-е изд. ─М.: Издательско-торговая корпорация «Дашков и К». 2005. ─336 с. [1]

2. Ярочкин, В.И. Информационная безопасность.– М.: Академический Проект. Мир. 2004. – 544 с.[2]

3. Проблема інформаційної безпеки // Спосіб доступу: URL http://ua.textreferat.com/referat-7941-6.html - Загол. з екрана[3]

4. Класифікація заходів із забезпечення інформаційної безпеки регіону/Спосіб доступу: URL: http://www.nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_1_2/251-254.pdf - Загол. з екрана[4]

5. Організаційні основи захисту інформації на підприємстві/Спосіб доступу: URL: http://bezopasnik.org/article/19.htm.- Загол. з екрана[5]