УДК 004.056

Д. С. Щур

МЕНЕДЖМЕНТ ПЕРСОНАЛУ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

Вінницький національний технічний університет

Анотація

Розглянуто принципи управління персоналом, поняття інформаційної безпеки, впровадження стандарту ISO 27001 в цілях підвищення безпеки конфіденціяльних даних .

Ключові слова: принципи управління персоналом, організаційна безпека, конфіденційна інформація, система управління інформаційною безпекою, ISO 27001.

Abstract

The principles of personnel management, the concept of information security, the implementation of the ISO 27001 standard in order to improve the security of confidential data are considered.

Keywords: principles of personnel management, organizational security, confidential information, information security management system, ISO 27001.

Вступ

У сучасному світі інформаційні технології розвиваються шаленими темпами, а з їх розвитком збільшується і кількість інформації, що використовується. У сучасних підприємствах майже кожен працівник стає носієм конфіденційної інформації, яка представляє інтерес для конкурентів та злочинних структур, також існує ризик завдання шкоди компанії через недбалість, безвідповідальність, банальне незнання правил роботи з конфіденційною інформацією та її захисту. Щоб такого не сталось, потрібний спеціальний підхід до менеджменту персоналу.

Основний зміст

Основними принципами управління персоналом для досягнення оптимальної захищеності інформації є: простий, оптимальний, науковий, прозорий, адаптивний та системний.

Науковий - формується на основі досягнень в науці зі сфери управління із врахуванням змін законів у розвитку економіки.

Простий – простіша система управління краще працює.

Оптимальний – багаторівневе розроблення варіантів для формування системи управління персоналом.

Прозорий - система управління персоналом має володіти концептуальною єдністю, включати єдину термінологію, діяльність всіх підрозділів і керівників повинно будуватися на єдиних конструкціях.

Адаптивний - можливість пристосування до змінюваних цілей організації.

Системний - передбачає, що управління персоналом охоплює всі категорії співробітників для вирішення проблем які виникають в діяльності працівника.

Важливою в організації управління також є організаційна безпека.

Організаційна безпека стосується не лише людей, а й процесів та процедур. Потрібно забезпечити, щоб працівники знали, що робити в певних ситуаціях, всі співробітники повинні розуміти свої ролі, обов'язки та процедури, яких вони повинні дотримуватися. Формалізована політика, курси, інструктажі мають вирішальне значення для забезпечення розуміння працівниками та дотримання вказівок з безпеки[1]. Для оптимізації управлінської функції керівництва компанії впроваджують системи контролю доступу.

Автоматизована система контролю доступу — електронна чи електронно-механічна система, що призначена для надання дозволу на прохід персоналу. Схожу систему можна спостерігати в метро [2].

Також керівництву було б доцільно впровадити стандарти з серії ISO 27001, адже дані стандарти були розроблені для систем управління інформаційною безпекою(СУІБ) [3]. Вони дозволяють зменшити втрати на підтримку та усунення загроз, контролювати небезпеки, мінімізувати ризики можливої шкоди, підвищити довіру та повагу як партнерів, так і користувачів інформаційних систем. Розглянемо стандарт

ISO 27001, він встановлює вимоги до створення, впровадження, і поліпшення систем менеджменту інформаційної безпеки, оцінки і обробки загроз.

1. Організація. Потрібно визначити внутрішні та зовнішні проблеми, які можуть вплинути на здатність підприємства створити систему управління інформаційною безпекою, наприклад, інформаційна безпека, а також юридичні, регулятивні та контрактні зобов'язання.

2. Сфера застосування. Інформація, визначена на першому кроці, використовується для документування сфери застосування СУІБ із зазначенням відповідних областей, а також меж. СУІБ потрібно впроваджувати, підтримувати та постійно вдосконалювати відповідно до конкретних ризиків захисту інформації та вимог ISO 27001. Сфера дії наголошує на важливості інтеграції СУІБ як частини загальної структури управління та процесу. Вимоги поширюються на всі організації, незалежно від типу, розміру чи галузі.

3. Лідерство. Керівництво створює політику інформаційної безпеки відповідно до стратегічного напрямку організації. Інтеграція СУІБ у стандартні організаційні процеси. Повідомлення деталей політики інформаційної безпеки та висвітлення важливості вимог СУІБ. Сприяння постійному вдосконаленню СУІБ. Забезпечення належної підтримки персоналу, який працює над удосконаленням системи.

4. Планування. План вирішення ризиків інформаційної безпеки повинен бути інтегрований у процес СУІБ, що передбачає 2 кроки. Перший - встановлення та застосування детального процесу управління ризиками інформаційної безпеки. Другий - Визначення та застосування процесу пом'якшення загроз, що включає засоби контролю, необхідні для реалізації кожного варіанту лікування ризику.

5. Підтримка. Підприємству потрібно отримати чи виділити ресурси, людей та інфраструктуру для ефективної реалізації СУІБ. Даний пункт передбачає навчання та наставництво персоналу для роботи з конфіденційною інформацією. Крім того, працівники повинні бути проінформовані про те, як вони можуть сприяти ефективності СУІБ, про наслідки невідповідності політиці захисту інформації. Нарешті, необхідно встановити внутрішню та зовнішню комунікаційну політику, що стосуються СУІБ

6. Операції. Цей крок зосереджений на виконанні планів та процесів, визначених у попередніх розділах. Організація повинна задокументувати всі дії, що проводяться, щоб забезпечити виконання процесів, як планувалося. Крім того, для визначення та контролю ризиків інформаційної безпеки необхідно визначити процеси, що передаються підрядниками.

7. Оцінка результативності. Оцінка ефективності забезпечує постійну ефективність та подальше вдосконалення СУІБ. Вона також регулярно визначає сфери потенційного вдосконалення інформаційної безпеки. Внутрішні аудити та огляди керівництва повинні проводитися та документуватися через визначені регулярні проміжки часу для оцінки ефективності СУІБ.

8. Вдосконалення. Невідповідність вимогам ISO 27001 потрібно усувати негайно після виявлення. Організаціям потрібно визначити та виконати кроки, щоб не повторювати ті самі проблеми. Крім того, підприємства повинні намагатись покращити придатність, адекватність та ефективність своїх СУІБ.

Висновок

В результаті даного дослідження було наведено інформацію про основні принципи менеджменту персоналу. Розкрито поняття організаційної безпеки. Досліджено загальну інформацію про стандарт ISO 27001. Розглянуто етапи впровадження даного стандарту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1.Організаційно-структурні аспекти створення і діяльності служби безпеки підприємства : веб-сайт URL: https://pidru4niki.com/84430/ekonomika/diyalnist_sluzhbi_bezpeki_pidpriyemstva. (дата звернення: 05.03.2021).

2.Система контролю доступу: веб-сайт URL: https://ukrinfosystems.com.ua/uk/design-and-construction/access-control-systems (дата звернення: 05.03.2021).

3.Стандарт ISO/IEC 27001:2013 : веб-сайт URL: https://intercert.com.ua/articles/posts/292-standart-iso-iec-27001-2013 (дата звернення: 05.03.2021).

Щур Дмитро Сергійович — студент групи 1Кі-17б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: baffer77@gmail.com

Shchur Dmytro S. — student group 1CE-17b, faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: baffer77@gmail.com