УДК 004.056.5:005.7

ПРОЦЕСНІ ПІДХОДИ ДО АУДИТУ СИСТЕМ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Євсюкова О.О.
Науковий керівник – к.т.н., доц. Добринін І.С.
Харківський національний університет радіоелектроніки
каф. ІКІ ім. В.В. Поповського,
м. Харків, Україна
тел. +380 98 853 34 57

Information security covers the tools and processes that organizations use to protect information. This includes policy settings that prevent unauthorized people from accessing business or personal information. Information system security services audit deal with the identification and analysis of potential risks, their mitigation or removal, with the aim of maintaining the functioning of the information system and the organization's overall business. While expanding online, cyber risks also increased with more targeted attacks against organizations ranging from small to large. Performing a security audit can help organizations by providing information related to the risks associated with their networks. It can also help in finding security loopholes and potential vulnerabilities in their system. Thereby patching them on time and keeping hackers at bay.

При створенні системи інформаційної безпеки важливим є процес перевірки та верифікації інформаційної безпеки, поряд з такими процесами, як впровадження захисних заходів, навчання персоналу та реалізація політики безпеки. Ці аудити дозволяють перевірити адекватність обраних захисних заходів та засобів та виявити існуючі вразливості в інформаційній системі. У процесі перевірки та верифікації інформаційної безпеки особливе місце займають аудити, основна мета яких – сформулювати незалежну оцінку інформаційної безпеки.

Процесний підхід – ефективний інструмент для аудиту систем менеджменту інформаційної безпеки, що ґрунтується на ідентифікації та оцінці процесів, що використовуються організацією для забезпечення безпеки інформації. Процесний підхід до аудиту фокусується на аналізі послідовності та взаємодії процесів, а також їх вхідних та вихідних даних. Він аналізує систему управління не як набір документованих процедур, а як активну систему процесів. Процесний підхід включає оцінку політики безпеки, процедур управління доступом, моніторингу та аналізу логів, управління ризиками та багато іншого.

Однією з переваг процесного підходу є його комплекність, адже такий підхід дає змогу оцінити ефективність системи інформаційної безпеки загалом, а не лише окремих її компонентів. Це дозволяє отримати повне уявлення про те, як організація забезпечує безпеку інформації. Аудитори,

які використовують процесний підхід, можуть виявити не тільки існуючі проблеми, а й потенційні ризики та вразливість системи безпеки.

Процесний підхід включає кілька етапів: ідентифікація та оцінка процесів, оцінка взаємозв'язків між процесами.

При ідентифікації процесів аудитор повинен визначити всі процеси, пов'язані із забезпеченням безпеки інформації в організації. Це можуть бути процеси управління доступом, резервного копіювання даних, моніторингу та аналізу логів, управління ризиками та інші процеси.

Наступним кроком аудитор повинен оцінити ефективність кожного процесу та виявити можливі вразливості та ризики у кожному з них. У цей момент може використовуватися стандарт ISO/IEC 27001, який містить рекомендації щодо оцінки процесів системи управління інформаційною безпекою.

При оцінюванні взаємозв'язків між процесами аудитор має визначити, як пов'язані між собою різні процеси та як вони впливають на безпеку інформації в організації. Аудитор повинен проаналізувати отримані результати та зробити висновки про те, наскільки ефективною є система менеджменту інформаційної безпеки в організації.

Серед недоліків процесного підходу аудиту систем менеджменту інформаційної безпеки виділяють його трудомісткість, високу складність та обмеженість. Такий підхід потребує великої кількості часу та ресурсів на ідентифікацію процесів, їх оцінку та аналіз взаємозв'язків між ними. Процесний підхід до аудиту інформаційної безпеки є складним методом, який потребує певних знань та навичок аудиторів. Процесний підхід може не враховувати деякі аспекти системи безпеки, які не є процесами, такими як фізична безпека та криптографічні методи захисту.

Проте, процесний підхід є одним із найефективніших методів оцінки системи менеджменту інформаційної безпеки. Результати аудиту, проведеного із застосуванням процесного підходу, можуть допомогти організації покращити свою систему менеджменту інформаційної безпеки та підвищити рівень захисту інформації.

Список використаних джерел:

1. ISO/IEC 27002:2022. http://www.itref.ir/uploads/editor/2ef522.pdf