УДК 006.065.3:006.015.8]:657.6

АНАЛІЗ НАЯВНИХ МЕТОДІВ АУДИТУ ФІЗИЧНИХ ОБ'ЄКТІВ ТА БЕЗПЕКИ ІНФРАСТРУКТУРИ

Пашкова А.В.
Науковий керівник – к.т.н., доц. Добринін І.С.
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського, м. Харків, Україна
тел. +38(099) 044-75-12

This work is devoted to the analysis of known methods for auditing physical security and infrastructure security. An audit of a physical facility is one of the first mandatory items when setting up a company's physical office. There are many different standards and the question is which one is better to choose. Therefore, an analysis of standards such as ISO / IEC 27002, ITAF, CIP-006 and NIST SP 800-53 has been carried out to find the most suitable one.

Проведення аудиту в компаніях має велике значення, оскільки це дозволяє переконатися у правильності та достовірності фінансової звітності, а також ефективності внутрішнього контролю та управління ризиками. Перше, з чого бажано починати при наявності фізичного офісу компанії, так це фізична безпека та безпека інфраструктури. Тому починати аудит слід саме з фізичної безпеки об'єкту, але стає питання: за яким саме стандартом проводити даний захід.

У роботі проведено аналіз стандарту Асоціації аудиту і контролю інформаційних систем, а саме ITAF (IT Audit Framework), який являє собою вичерпну еталонну модель використання кращих практик, яка встановлює стандарти, що описують ролі та обов'язки фахівців з аудиту, вимоги до проведення аудиту та звітності, методики планування, проведення та звітності за результатами аудиту. Однак після аналізу даного документу, було виявлено, що використання ITAF має багато переваг для організацій, які прагнуть підвищити рівень безпеки своїх інформаційних технологій та покращити якість своїх процесів. Однак ITAF не має достатньої документації для проведення аудиту фізичного об'єкта.

Проаналізовано також стандарт CIP-006 (Critical Infrastructure Protection – Physical Security) від North American Electric Reliability Corporation, який включає вимоги до підготовки та реагування на надзвичайні ситуації, контролю доступу, відеоспостереження та навчання персоналу. Мета CIP-006 – забезпечення захисту критичної інфраструктури від фізичних загроз та забезпечити безперервну роботу систем. Даний стандарт непогано описує фізичний захист об'єкту, але описує дуже докладно сам процес доступу, що не задовольняє цілям даної роботи.

Далі розглянуто міжнародно відомі стандарти ISO/IEC 27002 та NIST SP 800-53, описання проведено одночасно через схожість вимог щодо впровадження аудиту. Наприклад у NIST SP 800-53 є такі вимоги, як

конкретизація доступу без супроводу або посилення охорони в місцях де немає відеоспостереження. У стандарті ISO/IEC 27002 не окреслені дані можливості, тому доцільним буде додати дані пункти. Також цікавими є вимоги окремих вестибюлів або альтернативного робоче місця, що особливо актуально в Україні в даний час. Останнє, було додане, зі стандарту NIST SP 800-53, маркування компонентів. У ISO/IEC 27002 в розділі «Управління ресурсами СУІБ» є пункт про маркування, але він відноситься тільки до інформації, а не до апаратних компонентів. Щодо схожих пунктів, то до них можна віднести наявність фізичних бар'єрів, захист кабелів, окремі зони для транспортування/доставки та інше. Присутні вимоги, які через складнощі перекладу одразу не зрозумілі, поки не будуть розглянуті пояснення. Наприклад пункт корпусів, що замикаються, але при пояснені визначається, що це схоже на безпеку кабельних мереж у ISO/IEC 27002. Стосовно відсутніх пунктів у NIST SP 800-53 то це визначення периметру фізичної безпеки, наявність видимої ідентифікації персоналу, обмеження використання обладнання для запису у зонах безпеки, встановлення захисту від блискавки та інше.

Таким чином був проведений аналіз серед таких стандартів як ISO/IEC 27002, ITAF, CIP-006 та NIST SP 800-53. З цього можна зробити висновок, що у ITAF взагалі недостатньо вимог для проведення аудиту фізичного доступу об'єкту; стандарт CIP-006 має іншу мету, яка відрізняється від поставленої в даній роботі. Щодо NIST SP 800-53, то це непогана альтернатива стандарту ISO/IEC 27002, але являє собою більш грубий аналог ISO/IEC 27002. Тому було вирішено додати деякі вимоги з NIST SP 800-53, щоб покращити процес аудиту. Що стосується самого ISO/IEC 27002, то це найкращій варіант для обраної задачі, який має міжнародне визнання та який дуже поширений на території України.

Список використаних джерел:

1. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls. – URL: https://www.iso.org/standard/75652.html (дата звернення: 01.04.2023).

2. Wilbur L. Ross, Jr. (2020) NIST Secretary Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations. – URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf