УДК 004.056

А.С.Сухоребра
О.П.Войтович

РОЛЬ КІБЕРАУДИТУ В СУЧАСНИХ ІТ-ТЕХНОЛОГІЯХ

Вінницький національний технічний університет

Анотація
Зроблено огляд тенденцій розвитку кібераудиту та його важливість в сучасних ІТ-технологіях та бізнесі.
Ключові слова:кібераудит, сучасні ІТ-технології, стандарти, методи,бізнес.

Abstract
Overview of cyber audit trends and their importance in modern IT technologies and business.
Keywords: cyber audit, modern IT technologies, standards, methods, business.

Вступ

З появою перших комп'ютерів та доступу до мережі Інтернет, почала розвиватися й кіберзлочинність. Незлічити скільки було повідомлень про масштабні витоки персональних даних та втрати людьми грошей з власних рахунків. Одним зі способів вирішення подібних проблем є попередження їх виникнення, іншими словами, аудит безпеки на підприємстві.

Метою роботи є покращення безпеки малих підприємств шляхом проведення самоаудиту безпеки.

Результати дослідження

Під словом «ауди́т» сьогодні визначається перевірка даних бухгалтерського обліку і показників фінансової звітності суб'єкта господарювання [1]. Масштабне зростання кіберзлочинів та збитків завданих ними в сфері захисту інформації призвело до появи кібераудиту, що спрямований на попередження атак на інформаційно-комунікайні системи (ІКС) підприємства, шляхом перевірки застосованих заходів безпеки відповідно поширених стандартів [2].

Незважаючи на свою значимість на необхідність, він не користується популярністю. Це пояснюється неможливістю керівництва підприємства адекватно оцінити можливі ризики в разі кібератаки.

Для впровадження кібераудиту бажано мати системи, основані на міжнародних стандартах. Підготовчим етапом є застосування самоаудиту. Основними його перевагами є: визначення ресурсів для захисту, оцінка загроз і поточних заходів безпеки без втручання сторонніх людей та витрат коштів. Його реалізація відбувається за такими кроками, рис. 1:

Рисунок 1 – Етапи проведення самоаудиту

На основі отриманих в результаті самоаудиту даних, можна впроваджувати систему, побудовану на вже існуючих вимогах.

Зі зростанням загроз комп'ютерним мережам і даним, які обробляються було розроблено низку спеціалізованих стандартів, які визначають оцінку впроваджених заходів безпеки.

В залежності від специфікації підприємства існують такі стандарти:

- ITIL – найвідоміший посібник з управління IT-послугами. Дозволяє зрозуміти всім ,від IT-команди до керівництва бізнесом, загрози, які можуть виникнути при управлінні IT-послугами.
- PRINCE2 – структурований метод управління проектами в соціальній сфері.
- COBIT – підхід до управління інформаційними ресурсами. Затверджена методика процесів і практик з метою отримання максимальної вигоди від використання IT-технологій.
- PCI DSS – стандарт безпеки для платіжних карток. Використовують Visa, MasterCard, American Express, JCB та Discover.
- MOF – колекція практик, для досягнення максимальної надійності, доступності, підтримки в управлінні рішеннями та процесами в продуктах Microsoft.
- ISMS – система менеджменту інформаційної безпеки, яка основана на підході бізнес-ризиків при створенні, впровадженні, функціонуванні, моніторингу, аналізу, підтримці та покращенні інформаційної безпеки.
- ISO 27001 – є універсальним стандартом. Містить в собі вимоги для створення, розвитку та підтримки системи менеджменту інформаційної безпеки.

Головним недоліком стандартів є їх вузьконапрямленість, оскільки поодинці вони не зможуть повністю оцінити інформаційно-комунікаційну систему підприємства.

Висновки

Розглянуто основні методи аудиту, запропоновано самоаудит як засіб первинного аналізу стану безпеки на підприємстві.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про аудиторську діяльність [Електронний ресурс].-Режим доступу: URL: https://zakon.rada.gov.ua/laws/show/3125-12.- Назва з екрану.

2.Аудит кибербезопасности: больше, чем заполненный опросник [Електронний ресурс].-Режим доступу: URL: https://10guards.com/ru/articles/cybersecurity-audit/.- Назва з екрану.

3.Исскувство управления информационной безопасностью [Електронний ресурс].-Режим доступу: URL: http://www.iso27000.ru/standarty/iso-27000-mezhdunarodnye-standarty-upravleniya-informacionnoi-bezopasnostyu-1/.- Назва з екрану.

4. Conducting A Cyber Security Audit for Your Business [A How-To-Guide] [Електронний ресурс].-Режим доступу: URL: https://hackernoon.com/how-to-conduct-an-in-depth-cyber-security-audit-for-your-business-wgn33zym/.-Назва з екрану.

Сухоребра Ангеліна Сергіївна – студентка групи БС-17б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: suhorebraangelina@gmail.com

Войтович Олеся Петрівна – канд. техн. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет.

Suhorebra Anhelina S. - Department of Information Technology and Computer Engineering, Vinnitsa National Technical University, Vinnytsa, e-mail: suhorebraangelina@gmail.com

Voitovich Olesya P.- Cand. Sc. (Eng) Assistant Professor, Department of Information Protection, Vinnitsa National Technical University, Vinnytsa.