УДК 004.056

А. С. Сухоребра

МЕТОДИКА АУДИТУ ВІДПОВІДНО ДО NIST SP 800-53

Вінницький національний технічний університет

Анотація

Проаналізовано можливість виконання аудиту сучасними стандартами інформаційної безпеки. Зроблено огляд методики аудиту відповідно до стандарту NIST SP 800-53. Обгрунтовано важливість її автоматизації для використання в межах однієї організації чи підприємства.

Ключові слова: аудит, стандарти, NIST SP 800-53.

Abstract

The possibility of performing an audit by modern information security standards is analyzed. An overview of the audit methodology in accordance with the NIST SP 800-53 standard. The importance of its automation for use within one organization or enterprise is substantiated.

Keywords: audit, standards, NIST SP 800-53.

Вступ

Історія розвитку стандартів інформаційної безпеки бере свій початок 1990-го року. Саме тоді Міжнародна організація зі стандартизації (ISO) та Міжнародна електротехнічна організація (TEC) оголосили про створення спеціалізованої системи світової стандартизації. На цей час припадає поява перших стандартів ISO, в основу яких лягли критерії оцінки безпеки, розроблені фахівцями з Нідерланд, Франції, США, Великої Британії та Німеччини [1, 2]. Не дивлячись на стрімкий розвиток інформаційних технологій, різноманіття стандартів в цій галузі невелике. Не дивлячись на це, більшість з них зорієнтовані на державні підприємства або на великі сектори економіки, що унеможливлює їх використання малим чи середнім бізнесом. У 2005-му році було опубліковано перший примірник стандарту з аудиту NIST SP 800-53, який розроблявся спеціально для налагодження взаємодії між державними установами та малим бізнесом.

Метою роботи є покращення безпеки малих підприємств шляхом проведення аудиту безпеки на основі стандарту NIST SP 800-53.

Результати дослідження

Група спеціальних публікацій серії 800-х, від Інституту Стандартів США, спрямована на підвищення безпеки інформаційних систем та її співробітництва з урядом та академічними організаціями [3].

При вирішенні питань захисту інформації та конфіденційності кожна організація повинна дати відповідь на такі ключові питання:

– Які засоби безпеки та конфіденційності необхідні для задоволення вимог безпеки та конфіденційності?

– Чи були впроваджені вибрані засоби контролю та чи існує план, який це забезпечують?

– Який необхідний рівень впевненості, що вибраний засоби управління є ефективними?

Публікація 800-53 може допомогти організації дати відповіді на ці запитання. Вона забезпечує низку процедур для проведення оцінки заходів безпеки і приватності, що використовуються в федеральних інформаційних системах та організаціях. Процедури оцінки, що виконуються на різних фазах життєвого циклу розробки систем, несуперечливі з заходами забезпечення безпеки і приватності. Вони є настроювані та можуть бути легко адаптовані, щоб надати організаціям необхідну гнучкість, для проведення оцінки заходів безпеки.

Документ поділений на підрозділи, які називаються сім’ями. Кожна з них відповідає за певну область в забезпеченні інформаційної безпеки (ІБ). Всього в стандарті представлено 17 сімейств, відображають всю глибину ІБ в організації: від аудиту до безпеки персоналу та керування програмою ІБ. Наприклад: обізнаність та навчання (AT), аудит і звітність (AU), авторизація та оцінка безпеки

(CA), планування безперервності бізнесу (CP), ідентифікація та автентифікація (IA), реагування на інциденти (IR) тощо.

Методика аудиту побудована у вигляді багаторівневої піраміди, в основі якої лежить політика інформаційної безпеки та керування обліковими записами.

Важливість автоматизації проведення аудиту полягає в знятті навантаження на людський ресурс. Всі відомий факт, що вразливість будь-якої інформаційної системи – людина. Хоч вона й є невід'ємною частиною , оскільки приймає безпосередньо участь в її створенні.

Відомий метод CRAMM, використовуваний британським урядом являє собою опитувальник, що містить в собі близько 600 питань, пов'язаних з поточним рівнем безпеки, ризиками та їх величиною та виборі методів захисту [2, 4]. Значно ускладнить життя аудитору купа паперу з надрукованими питаннями такого спрямування. Така одноманітна робота через декілька годин призведе до підвищення імовірності помилки аудитора, через втому.

Для полегшення такого громіскткого процесу кращим рішенням є створення застосунку на основі бази даних, з можливістю автоматизації деяких процесів обробки та агрегації даних, а також генерування остаточного звіту для обрису всієї ситуації в цілому. В наслідок такої автоматизації очікується результат аналогічний отриманому в [5] для оцінювання інформаційної безпеки – це сприятиме пришвидшенню проведення процесу аудиту та дасть змогу для керівництва точно визначити слабкі місця та напрямки покращення в інформаційній безпеці свого підприємства чи організації шляхом аналізу динаміки зміни показників за певні проміжки часу.

Висновки

Було розглянуто можливість автоматизації проведення аудиту для підприємств малого та середньо бізнесу методикою, представленою в стандарті NIST SP 800-53. Проведений аналіз показав доцільність автоматизації процесу аудиту.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Безопасность ИТ: общих стандартов мало. URL: https://www.cnews.ru/reviews/free/security2004/standard/ (дата звернення 02.03.2021)
2. Сухоребра А. С., Войтович О. П. Роль кібераудиту в сучасних IT-технологіях. в Матеріали конференції «XLIX Науково-технічна конференція підрозділів Вінницького національного технічного університету (2020)», Вінниця, 2020. С. 1219-1220 URL: https://conferences.vntu.edu.ua/index.php/allvntu/index/pages/view/zbirn2020 (дата звернення: 04.03.2021)
3. Security and Privacy Controls for Information Systems and Organizations/ URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (дата звернення 02.03.2021)
4. Современные методы и средства анализа и управление рисками информационных систем компаний. URL: http://citforum.ru/products/dsec/cramm/#:~:text=%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%20CRAMM%20(CCTA%20Risk%20Analysis,%D0%B2%D0%BE%D0%BE%D1%80%D1%83%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5%20%D0%B2%20%D0%BA%D0%B0%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%B5%20%D0%B3%D0%BE%D1%81%D1%83%D0%B4%D0%B0%D1%80%D1%81%D1%82%D0%B2%D0%B5%D0%BD%D0%BD%D0%BE%D0%B3%D0%BE%20%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%B0. (дата звернення 03.03.2021)
5. Дудатьєв А.В., Баришев Ю.В. Редактор дерева ризику-відмов. *Інформаційні технологій та комп'ютерна інженерія*. 2007. №1. С. 86-89.

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

Науковий керівник: **Баришев Юрій Володимирович** – к. т. н. доцент кафедри захисту інформації, , Вінницький національний
технічний університет, Вінниця

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

Scientific supervisor: **Yurii Baryshev** – PhD (Eng), Associated Professor of Information Protection Department, Vinnytsia National Technical University, Khmelnytske shosse 95, Vinnytsia, Ukraine, email: yuriy.baryshev@vntu.edu.ua