Герасимов Є.В., Асп (152)-22, Христич В.П., Асп (175)-23, Нос Р.С., Асп (175)-23

РОЗВИТОК КВАЛІМЕТРИЧНИХ ПІДХОДИ ДО ОЦІНЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

Методи кваліметричного оцінювання інформаційної безпеки на підприємстві включають в себе ряд інструментів та підходів, які дозволяють оцінити рівень безпеки інформації на підприємстві. Ось декілька з найбільш поширених методів:

Метод оцінки ризиків: Цей метод включає в себе ідентифікацію потенційних загроз і ризиків для інформаційної безпеки на підприємстві. Визначаються ймовірність виникнення загроз і потенційні наслідки. Після цього проводиться оцінка ризиків, і визначаються пріоритети для заходів з підвищення безпеки.

Метод аналізу уразливостей: Цей метод передбачає виявлення уразливостей в системах та мережах підприємства. Проводиться сканування та аудит систем для виявлення можливих слабких місць. Після чого розробляються заходи для усунення уразливостей.

Метод оцінки активів: В цьому методі проводиться ідентифікація важливих інформаційних активів на підприємстві. Для кожного активу визначаються його вартість та важливість для підприємства. Це допомагає визначити, на які активи слід акцентувати увагу для підвищення їхньої безпеки.

Метод оцінки ефективності заходів забезпечення інформаційної безпеки: Після впровадження заходів з підвищення безпеки проводиться оцінка їх ефективності. Це дозволяє визначити, чи були досягнуті поставлені цілі та які зміни відбулися в рівні безпеки.

Метод оцінки резервів підвищення інформаційної безпеки: Цей метод передбачає визначення можливостей для підвищення безпеки на підприємстві. Розглядаються нові технології та підходи, які можуть бути використані для покращення інформаційної безпеки.

Ці методи можуть застосовуватися окремо або в поєднанні, залежно від потреб та специфіки підприємства. Вони допомагають здійснити комплексну оцінку інформаційної безпеки та розробити стратегію для її підвищення.

NIST (National Institute of Standards and Technology) Cybersecurity Framework - це набір керівних рекомендацій та стандартів, розроблених національним інститутом США з метою покращення кібербезпеки організацій та захисту їхніх інформаційних активів. Цей фреймворк допомагає підприємствам та урядовим організаціям розробити та впровадити ефективні стратегії кібербезпеки, виявити ризики та розробити заходи для їх зменшення.

NIST Cybersecurity Framework складається з п'яти ключових елементів:

1. **Цільовість (Function)**: Визначення основних цілей та завдань кібербезпеки, включаючи ідентифікацію, захист, виявлення, реагування та відновлення.
2. **Категорії (Category)**: Розподіл завдань кібербезпеки на конкретні категорії, такі як ідентифікація або захист, ідентифікація конкретних дій та контролів.
3. **Підкатегорії (Subcategory)**: Розгортання конкретних завдань та контролів, пов'язаних з категоріями.
4. **Контролі (Control)**: Опис конкретних технічних та організаційних заходів для забезпечення кібербезпеки.

5. **Практики (Practices)**: Рекомендації та кращі практики для впровадження контролів та стратегій кібербезпеки.

NIST Cybersecurity Framework допомагає організаціям оцінити їхню поточну кібербезпеку, розробити плани покращення та визначити, які контролі та заходи кібербезпеки слід впровадити для досягнення бажаних рівнів безпеки. Він широко використовується як інструмент для керівництва та підтримки впровадження кібербезпеки в різних галузях і організаціях.

Використання методологій, таких як ISO 27001 або NIST Cybersecurity Framework, для ідентифікації потенційних загроз, визначення вразливостей та оцінки можливих наслідків порушень інформаційної безпеки включає наступні кроки: Вибір методології (ISO 27001 та NIST Cybersecurity Framework - це дві з найбільш визнаних та використовуваних стандартів, вибір залежатиме від специфічних потреб та вимог підприємства); Ініціювання процесу оцінки; Ідентифікація загроз; Визначення вразливостей; Оцінка наслідків порушень; Розробка стратегій управління ризиками; Моніторинг і підтримка.

Використання таких методологій допомогає підприємству ідентифікувати і керувати ризиками, пов'язаними з інформаційною безпекою, та покращити загальний рівень захисту даних і систем.

Література:

1. Методика управління ризиками для системи управління якістю при виготовленні виробів медичного призначення // А.М. Денисенко, В.М. Бурдейна, Ю.С. Лис - Системи управління, навігації та зв'язку, 2019, випуск 3(55). – С.25 – 30. http://journals.nupp.edu.ua/sunz/article/view/1549

2. Trishch, R., Nechuiviter, O., Hrinchenko, H., Bubela, T., Riabchykov, M., Pandova, I. (2023) Assessment of safety risks using qualimetric methods. MM Science Journal. October 2023, 6668. DOI: https://doi.org/10.17973/MMSJ.2023_10_2023021

3. Черняк О. М., Лис Ю. С., Грінченко Г. С., Каницька І. В. Багатокритеріальне оцінювання умов праці на виробництві. Вісник Національного технічного університету «ХПІ». Серія: Нові рішення в сучасних технологіях. – Харків: НТУ «ХПІ». 2020. № 3 (5). С. 28-33.

4. Грінченко Г.С., Тріщ Ю.В., Грінченко В.В., Багаєв І.О., Фатєєва Л.Ю. Підходи щодо оцінювання ризиків функціонування систем об’єктів різного призначення. Машинобудування: Збірник наукових праць. 2022. №29. С. 70 -79. DOI 10.32820/2079-1747-2022-29-70-79

Під керівництвом: доц. каф. АМЕТ, Г.С. Грінченко