НОРМАТИВНО-ПРАВОВЕ ОТОЧЕННЯ ПРОЕКТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Шевчук Костянтин, Пінтяк Олександр, Смирнов Дмитро
Одеський національний політехнічний університет
Україна, Одеса
kis.shevchuk@gmail.com

Забезпечення інформаційної безпеки є дуже важливим етапом в розробці будь-яких програм, комп'ютерних систем і мереж. При їх розробці можна обмежитися міжнародними стандартами, загальними критеріями оцінки безпеки інформаційних технологій, практичними правилами управліннями.

Ключові слова: управління, програмами, інформаційної, безпеки, міжнародні, стандарти

Проблема забезпечення безпеки інформаційних технологій займає все більш значне місце в реалізації комп'ютерних систем і мереж у міру того, як зростає їх роль у розвитку інформатизації суспільства.

Забезпечення безпеки інформаційних технологій являє собою комплексну проблему, яка вирішується в напрямках вдосконалення правового регулювання застосування інформаційних технологій, вдосконалення методів і засобів їх розробки, розвитку системи сертифікації, забезпечення відповідних організаційно-технічних умов експлуатації.

Найбільш значущими нормативними документами, що визначають критерії оцінки захищеності і вимоги, що пред'являються до механізмів захисту, є «Загальні критерії оцінки безпеки інформаційних технологій» (The Common Criteria for Information Technology Security Evaluation/ISO 15408) і «Практичні правила управління безпекою інформації» (Code of practice for Information security management/ISO 17799).

Найбільш повні критерії для оцінки механізмів безпеки організаційного рівня представлені в ISO 17799, прийнятому в 2000 році. Цей стандарт, є міжнародною версією британського стандарту BS 7799, містить практичні правила управління безпекою і може використовуватися в якості критеріїв оцінки механізмів безпеки організаційного рівня, включаючи адміністративні, процедурні та фізичні заходи захисту.

Практичні правила поділені на десять розділів:

1. Політика безпеки.
2. Організація захисту.
3. Класифікація ресурсів та їх контроль.
4. Безпека персоналу.

5. Фізична безпека.
6. Адміністрування комп'ютерних систем і мереж.
7. Контроль доступу.
8. Розробка та супровід інформаційних систем.
9. Планування безперебійної роботи організації.
10. Контроль виконання вимог політики безпеки.

Десять ключових засобів контролю (механізмів управління інформаційною безпекою), пропонованих в ISO 17799, вважаються особливо важливими. При використанні деяких засобів контролю, наприклад, шифрування, можуть знадобитися поради фахівців з безпеки та оцінка ризиків.

Для забезпечення захисту особливо цінних ресурсів або надання протидії особливо серйозним загрозам безпеці, у ряді випадків можуть знадобитися більш сильні засоби контролю, які виходять за рамки ISO 17799.

Ключові засоби контролю являють собою або обов'язкові вимоги (наприклад, вимоги чинного законодавства), або вважаються основними структурними елементами інформаційної безпеки (наприклад, навчання правил безпеки).

Ці кошти актуальні для всіх організацій і складають основу системи управління інформаційною безпекою. Вони служать в якості основи для організацій, приступають до реалізації засобів управління інформаційною безпекою. До ключових віднесено такі засоби контролю:

- документ про політику інформаційної безпеки; розподіл обов'язків щодо забезпечення інформаційної безпеки;
- навчання та підготовка персоналу до підтримки режиму інформаційної безпеки; повідомлення про випадки порушення захисту;
- комплектний засіб захисту від вірусів;
- планування безперебійної роботи організації;
- контроль над копіюванням програмного забезпечення, захищеного законом про авторське право;
- захист документації організації;
- захист даних;
- контроль відповідності політиці безпеки.

Процедура аудиту безпеки автоматизованих систем за стандартом ISO 17799 включає в себе перевірку наявності перелічених ключових засобів контролю, оцінку повноти та правильності їх реалізації, а також аналіз їх адекватності ризикам, існуючим у даній середовищі функціонування. Складовою частиною робіт з аудиту також є аналіз і управління ризиками.

ДЖЕРЕЛА

6. ISO/IEC 17799:2005. URL: https://www.iso.org/standard/39612.html
7. ISO/IES 15408-1:2009. URL: https://www.iso.org/standard/50341.html