Міжнародні стандарти інформаційної безпеки

Стандарти інформаційної безпеки — це стандарти, які надають рекомендації щодо розробки та експлуатації інформаційних систем з питань керування інформаційною безпекою, захисту від несанкціонованого доступу, кібербезпеки, криптографічного захисту інформації, захисту персональних даних. Загальні (рамкові) стандарти можуть доповнюватись галузевими стандартами (спеціальні вимоги у медичній, авіакосмічній, автомобільній, фінансовій галузях) та стандартами щодо безпечного використання певних технологій (наприклад хмарних обчислень).

Стандарти кібербезпеки

Це методи, що зазвичай викладені в опублікованих матеріалах, які намагаються захистити кібернетичне середовище користувача чи організації. Це середовище включає в себе користувачів, мережі, пристрої, все програмне забезпечення, процеси, інформацію в режимі зберігання або транзиту, програми, служби та системи, які можуть бути безпосередньо або опосередковано підключені до мереж. Основна мета — знизити ризики, включаючи попередження або пом'якшення кібер-атак. Ці опубліковані матеріали включають збірки інструментів, політику, концепції безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, навчання, найкращі практики, забезпечення та технології.

> **Міжнародна організація зі стандартизації** (англ. International Organization for Standardization, **ISO**) — міжнародна організація, метою діяльності якої є ратифікація стандартів, розроблених спільними зусиллями делегатів від різних країн.
>
> Організація ISO була заснована 23 лютого 1947 р. двадцятьма п'ятьма національними організаціями зі стандартизації, як координаційний орган.

Чому компаніям потрібно дотримуватися стандартів інформаційної безпеки

Існує кілька ключових причин, чому компаніям вигідно дотримуватися інформаційних стандартів:

- Досягнення відповідності нормативним вимогам: Дотримання стандартів інформаційної безпеки призводить до того, що компанії стають відповідними до вимог IT-безпеки, необхідних для їхньої галузі. Як наслідок, вони можуть уникнути негативних наслідків невідповідності, таких як фінансові штрафи та юридичні проблеми.
- Запобігання кібератак: Стандарти інформаційної безпеки визначають найкращі практики кібербезпеки, тому їхнє дотримання є ефективним способом для компаній підходити до

своїх потреб у інформаційній безпеці. Це пов’язано з тим, що дотримання стандартів IT-безпеки вимагає від компанії реалізації необхідних заходів, процесів, політик і заходів контролю, які покращать її позицію в кібербезпеці. Тепер, хоча важливо зазначити, що відповідність не обов’язково означає безпеку, оскільки кіберзагрози розвиваються швидше, ніж стандарти безпеки, це відмінна вихідна точка.
- Підвищена обізнаність про ризики: Дотримання стандартів безпеки вимагає від команд безпеки компанії підвищення обізнаності про найкращі практики кібербезпеки, визначення, термінологію та, найголовніше, про весь спектр кіберзагроз, з якими вони стикаються. Це зменшує ймовірність дорогих порушень через незнання та зменшує потребу в методі проб і помилок для пом’якшення кібератак.
- Підвищення репутації: Дотримання стандартів інформаційної безпеки демонструє прихильність вашої компанії до кібербезпеки та забезпечення безпеки даних, особливо коли ви отримуєте сертифікацію за свої зусилля. Це вселяє впевненість у існуючих і потенційних клієнтів, партнерів по ланцюжку поставок тощо, і заспокоює їх, що їхня інформація безпечна при роботі з вами.

Два основні стандарти інформаційної безпеки

Два основні стандарти інформаційної безпеки, яких компанії прагнуть дотримуватися, це **ISO 27001** і **ISO 27002**. Їх видає Міжнародна організація зі стандартизації (ISO) - незалежний міжнародний орган, який створює стандарти, що охоплюють технології, виробництво, управління та інше. ISO 27001 і 27002 є двома ключовими стандартами з серії ISO 27000, яка складається з понад 45 стандартів, що охоплюють широкий спектр питань інформаційної безпеки.

ISO 27001 - це стандарт інформаційної безпеки, який визначає вимоги до того, як компанія повинна реалізувати систему управління інформаційною безпекою (ISMS).

ISMS - це рамка управління, яка містить структурований набір заходів, що дозволяє компанії керувати своїми ризиками інформаційної безпеки.

ISO 27001 визначає засоби контролю та процедури, які вам потрібно реалізувати в межах вашої ISMS для пом’якшення ризиків інформаційної безпеки, характерних для вашої компанії, а також як контролювати та вимірювати постійну ефективність і продуктивність зазначених заходів контролю. Компанії, яким потрібне всебічне керівництво щодо покращення їхньої позиції в інформаційній безпеці, можуть значно скористатися тим, як ISO 27001 зручно консолідує необхідні політики, процеси та засоби контролю.

Компанія може довести свою відповідність стандарту ISO 27001 за допомогою аудитів і сертифікації, які надаються акредитованими ISO агентствами.

Джерела

- Стандарти інформаційної безпеки
- Міжнародна організація зі стандартизації
- Information security standards - an overview I DQS
- What Are Information Security Standards?