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

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.

ISO 27002

Хоча ISO 27001 надає детальні рекомендації щодо розробки системи управління інформаційною безпекою (ISMS), він фактично не вимагає формально, які конкретні контролі інформаційної безпеки повинна реалізувати компанія. Це пов’язано з тим, що необхідні контролі можуть відрізнятися залежно від конкретних потреб компанії в інформаційній безпеці. Саме тут і вступає в дію ISO 27002.

ISO 27002 доповнює ISO 27001 і деталізує контролі інформаційної безпеки, які може реалізувати компанія, як зазначено в ISO 27001. Компанії можуть реалізувати будь-які контролі, які найбільш підходять для їхніх конкретних ризиків інформаційної безпеки; ISO 27002 надає найкращі практики для вибору, реалізації та управління цими контролями, враховуючи ризикове середовище компанії.

Контролі, деталізовані в ISO 27002, такі ж, як описані в Додатку A до ISO 27001. Хоча раніше як ISO 27002, так і Додаток A містили 114 контролів, оновлене видання 2022 року було реорганізовано в 93 контролі, з яких 58 оновлено, 24 об’єднано та 11 зовсім нових. Аналогічно, хоча 114 контролів були розподілені по 14 доменах, оновлення 2022 року передбачає розподіл 93 контролів по наступним чотирьом категоріям:

- Організаційні
- Людські
- Фізичні
- Технологічні

Крім того, на відміну від ISO 27001, для доведення відповідності не потрібна сертифікація. Це тому, що ISO 27002 є інформативним, а не нормативним стандартом, як ISO 27001. Іншими словами, метою ISO 27002 є детальніший опис необхідних контролів, а не їхнє призначення, як це має місце в ISO 27001.

Які проблеми виникають, якщо не дотримуватися стандартів IT-безпеки?

Ми розглянули кілька переваг дотримання стандартів інформаційної безпеки, але що станеться, якщо ви не дотримуватиметеся їх? Ось найбільш помітні наслідки невиконання стандартів IT-безпеки:

- Збільшений ризик порушення безпеки: оскільки стандарти безпеки визначають найкращі практики для пом’якшення ризиків кібербезпеки та забезпечення безпеки інформації, недотримання їх ставить вас під загрозу дорогої атаки.
- Юридичні проблеми: недотримання стандартів IT може призвести до того, що ви не будете відповідати галузевим або урядовим нормативним актам, що може призвести до судових позовів проти вашої компанії, особливо у разі порушення даних. Крім того, ваша компанія може бути оштрафована на значні суми.
- Штрафи: крім юридичних проблем, ваша компанія може бути оштрафована на значні суми за невиконання вимог. Крім того, з деякими IT-стандартами, такими як GDPR (Загальний регламент про захист даних), вас можуть зобов’язати компенсувати будь-яку шкоду, завдану в результаті порушення.

- Пошкодження репутації: хоча компанія може подолати юридичні проблеми та фінансові труднощі, пошкодження репутації важче відновити. Якщо ваші клієнти не вважають, що їхні дані безпечні у вашій компанії, вони шукатимуть інші варіанти. Аналогічно, якщо ваша компанія має погану репутацію в області безпеки, завоювання довіри, необхідної для залучення нових клієнтів, буде складним завданням.

Інші стандарти інформаційної безпеки

GDPR (General Data Protection Regulation)

Загальний регламент про захист даних (англ. General Data Protection Regulation, GDPR; Regulation (EU) 2016/679) — регламент в межах законодавства Європейського Союзу щодо захисту персональних даних усіх осіб у межах Європейського Союзу та Європейської економічної зони. Він також стосується експорту персональних даних за межі ЄС і ЄЕЗ. GDPR покликаний насамперед надати громадянам та резидентам ЄС контроль за їхніми персональними даними та спростити регуляторне середовище для міжнародного бізнесу шляхом уніфікації регулювання в межах ЄС.

PCI DSS

Payment Card Industry Data Security Standard (PCI DSS) — стандарт безпеки даних індустрії платіжних карток, розроблений Радою зі стандартів безпеки індустрії платіжних карток (Payment Card Industry Security Standards Council, PCI SSC), заснованою міжнародними платіжними системами Visa, MasterCard, American Express, JCB і Discover[1)]). Стандарт являє собою сукупність 12 деталізованих вимог щодо забезпечення безпеки даних про власників платіжних карток, які передаються, зберігаються і обробляються в інформаційних інфраструктурах організацій. Прийняття відповідних заходів щодо забезпечення відповідності вимогам стандарту представляє комплексний підхід до забезпечення інформаційної безпеки даних платіжних карток.

NIST

Націона́льний інститу́т станда́ртів і технолóгії (NIST, до 1988 відомий як Національне бюро стандартів, англ. National Bureau of Standards. NBS) — національний орган зі стандартизації у США.

NIST — неурядова некомерційна організація, що координує роботи з добровільної стандартизації в приватному секторі економіки, керує діяльністю організацій-розробників стандартів і приймає рішення про надання стандарту статусу національного (якщо в ньому зацікавлені різні фірми і стандарт набуває міжгалузевого характеру).

Джерела

- Стандарти інформаційної безпеки
- Міжнародна організація зі стандартизації
- Information security standards - an overview I DQS
- What Are Information Security Standards?
- Національний інститут стандартів і технології
- Загальний регламент про захист даних
- PCI DSS

1)

Frequently Asked Question. PCI Security Standards Council (амер.