2.33.

**інформаційна безпека**

збереження конфіденційності (2.12), цілісності (2.40) та можливості застосування (2.9) інформації

Примітка 1 до визначення: Крім того, можуть використовуватися інші властивості, такі як справжність (2.8), контрольованість, неспростовність авторства (2.54) та надійність (2.62).

2.34

**неперервність інформаційної безпеки**

процеси (2.61) та процедури, які гарантують постійне забезпечення інформаційної безпеки (2.33)

2.35

**подія інформаційної безпеки**

встановлене виникнення стану системи, служби або мережі, що вказує на можливе порушення політики (2.60) інформаційної безпеки (2.33) або збій в роботі засобів управління (2.16), або на раніше невідому ситуацію, яка може мати відношення до безпеки

2.36

**інцидент інформаційної безпеки**

одне або декілька небажаних або несподіваних подій інформаційної безпеки (2.35), які зі значним ступенем імовірності піддають небезпеці ділову діяльність та загрожують інформаційній безпеці (2.33)

2.37

**менеджмент інцидентів інформаційної безпеки**

процеси (2.61) виявлення, інформування, оцінки, реагування, обробки та лікування уроків з інцидентів інформаційної безпеки (2.36)

2.38

**спільнота обміну інформації**

група організацій (2.57), які досягли угоди про спільне використання інформації

Примітка 1 до визначення: В якості організації (2.57) може виступати окрема особа

2.39

**інформаційна система**

застосунки, служби, активи, які пов’язані з інформаційними технологіями, або інші компоненти обробки інформації

2.40

**цілісність**

властивість збереження повноти та точності

2.41

**зацікавлена сторона**

особа або організація (2.57), які можуть впливати на рішення або дію, а також на яких можуть впливати або вони припускають, що на них можуть впливати рішення або дії

2.42

**внутрішній контекст**

внутрішнє середовище, в якому організація (2.57) прагне досягти своїх цілей

Примітка 1 до визначення: Внутрішній контекст може включати:

* органи управління, організаційну структуру, ролі та зобов’язання;
* політики (2.60), цілі (2.56) та стратегії, які застосовуються для їх досягнення;
* можливості, що розуміються в термінах ресурсів та накопичених знань (наприклад, капітал, час, персонал, процеси (2.61), системи та технології);
* інформаційні системи (2.39), інформаційні потоки та процеси (2.56) прийняття рішень (як формалізовані, так і не формалізовані);
* взаємовідносини з внутрішніми впливаючими сторонами (2.82), їх думки та цінності;
* корпоративна культура організації (2.57);
* стандарти, керівництва та моделі, прийняті організацією (2.57);
* форма та об’єм договірних відношень.

2.43

**проект СУІБ**

структуровані дії, що робить організація (2.57) для впровадження СУІБ

2.44

**рівень ризику**

величина ризику (2.68), що виражається комбінацією наслідків (2.14) та їх ймовірності (2.45)