Безпека інформаційних технологій

Інформаційна безпека — це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, використання й розвиток в інтересах громадян або комплекс заходів, спрямованих на забезпечення захищеності інформації особи, суспільства і держави від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення (у цьому значенні частіше використовують термін «захист інформації»).

Інформація - це відомості про об'єкти, процеси, явища, події, які мають значення для суб'єкта.

Інформаційна система - це сукупність взаємопов'язаних засобів, методів і процедур, що забезпечують автоматизоване створення, обробку, зберігання, передачу, використання інформації.

Інформаційна безпека держави характеризується ступенем захищеності і, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості і т.д.) стосовно небезпечних (дестабілізаційних, деструктивних, суперечних інтересам країни тощо), інформаційним впливам, причому як до впровадження, так і до вилучення інформації.

Поняття інформаційної безпеки не обмежується безпекою технічних інформаційних систем чи безпекою інформації у чисельному чи електронному вигляді, а стосується усіх аспектів захисту даних чи інформації незалежно від форми, у якій вони перебувають.

Об'єктивно категорія «інформаційна безпека» виникла з появою засобів інформаційних комунікацій між людьми, а також з усвідомленням людиною наявності у людей і їхніх співтовариств інтересів, яким може бути завдано збитку шляхом дії на засоби інформаційних комунікацій, наявність і розвиток яких забезпечує і задає інформаційний обмін між всіма елементами соціуму.

Основні поняття безпеки інформаційних технологій

- **Несанкціонований доступ** - це будь-які дії, що призвели до отримання інформації особою, яка не має на це права.
- **Використання** - це будь-які дії, що призвели до використання інформації особою, яка не має на це права.
- **Модифікація** - це будь-які дії, що призвели до зміни інформації особою, яка не має на це права.
- **Знищення** - це будь-які дії, що призвели до втрати інформації особою, яка не має на це права.
- **Блокування** - це будь-які дії, що призвели до тимчасового припинення доступу до інформації особою, яка має на це право.
- **Копіювання** - це будь-які дії, що призвели до створення копії інформації особою, яка не має на це права.
- **Поширення** - це будь-які дії, що призвели до передачі інформації особі, яка не має на це права.

Властивості інформації

1. Конфіденційність: Захист інформації від несанкціонованого доступу. Це означає, що лише авторизовані особи мають доступ до конфіденційної інформації.
2. Цілісність: Забезпечення недопущення несанкціонованої зміни або руйнування інформації. Інформація повинна залишатися недоторканою і незмінною.
3. Доступність: Забезпечення доступності інформації для авторизованих користувачів. Інформація повинна бути доступною тоді, коли її потрібно використовувати.
4. Аутентифікація: Перевірка ідентичності користувачів і систем для забезпечення, що доступ надається тільки авторизованим особам.
5. Авторизація: Надання прав на доступ до певної інформації або ресурсів конкретним користувачам на підставі їхніх ролей та обов'язків.
6. Аудит: Запис та моніторинг дій користувачів та систем для виявлення незвичайних або підозрілих активностей.
7. Фізична безпека: Заходи для захисту фізичного доступу до інформації, такі як обмеження доступу до приміщень та обладнання.
8. Криптографія: Використання шифрування для захисту інформації від несанкціонованого доступу під час передачі чи зберігання.
9. Захист від загроз: Виявлення, аналіз і запобігання загрозам для інформаційної безпеки, таким як віруси, хакерські атаки, фішинг та інші.

Критерії

Критерії оцінки інформаційної безпеки (англ. Common Criteria) є методологічною базою для визначення вимог захисту комп'ютерних систем від несанкціонованого доступу, створення захисних систем та оцінки ступенів захищеності.

З допомогою критеріїв можливо порівняти різні механізми захисту інформації та визначити необхідну функціональність таких механізмів у розробці захищених комп'ютерних систем.

Для характеристики основних критеріїв інформаційної безпеки застосовують модель тріади **CIA**:

1. Конфіденційність (англ. **C**onfidentiality) — властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем
2. Цілісність (англ. **I**ntegrity) — означає неможливість модифікації неавторизованим користувачем
3. Доступність (англ. **A**vailability) — властивість інформації бути отриманою авторизованим користувачем, за наявності у нього відповідних повноважень, в необхідний для нього час

Інформаційні системи аналізуються в трьох головних секторах: **технічних засобах, програмному забезпеченні і комунікаціях**, з метою ідентифікування і застосування промислових стандартів інформаційної безпеки, як механізми захисту і запобігання, на трьох рівнях або шарах: фізичний, особистий і організаційний. По суті, процедури або правила запроваджуються для інформування адміністраторів, користувачів та операторів щодо використання захисної продукції для гарантування інформаційної безпеки в межах організацій.

> **Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України** прийняв нормативний документ технічного захисту інформації 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». **НД ТЗІ 2.5-004** було розроблено на основі *Canadian Trusted Computer Product Evaluation Criteria* (CTCPEC) (т. зв. Канадських критеріїв), який також було використано при розробці Common Criteria.

Принципи забезпечення інформаційної безпеки

Принципи забезпечення інформаційної безпеки містять:

- законність, баланс інтересів особи, суспільства і держави;
- комплексність;
- системність;
- інтеграція з міжнародними системами безпеки;
- економічна ефективність.

Неможливо створити систему, захист якої не можна буде зламати, основним принципом може бути створення такого механізму захисту, вартість злому якого буде дорожчою за інформацію, яку можна отримати. Тому необхідним є впровадження програмних засобів безпеки, які вмонтовані до складу програмного забезпечення системи і є потрібними для виконання функцій захисту. В сучасних умовах, не гарантуючи належний захист інформації, не можливо забезпечити стабільний економічний розвиток як окремого підприємства, так і держави.

Законодавчі вимоги і регулювання інформаційної безпеки

Інформаційна безпека є важливою складовою національної безпеки України. Для забезпечення інформаційної безпеки в Україні діє законодавство, яке включає в себе:

- Конституцію України, яка в статті 32 гарантує право громадян на інформацію.
- Закон України “Про основні засади забезпечення кібербезпеки України”, який визначає правові та організаційні засади забезпечення кібербезпеки України.
- Закон України “Про захист персональних даних”, який визначає правові та організаційні засади захисту персональних даних.
- Закон України “Про інформацію”, який визначає правові та організаційні засади забезпечення права громадян на інформацію.
- Інші нормативно-правові акти, які регулюють питання інформаційної безпеки.

Законодавство України в галузі інформаційної безпеки спрямоване на:

- Захист інформації від несанкціонованого доступу, використання, модифікації, знищення, блокування, копіювання, поширення та інших неправомірних дій.
- Забезпечення конфіденційності, цілісності та доступності інформації.
- Захист персональних даних від неправомірного використання та поширення.
- Забезпечення інформаційної безпеки в Інтернеті.

Закон України "Про основні засади забезпечення кібербезпеки України" визначає наступні основні принципи забезпечення кібербезпеки:

- **Стабільність** - забезпечення сталого функціонування інформаційних систем і мереж, а також захисту інформації від несанкціонованого доступу, використання, модифікації, знищення, блокування, копіювання, поширення та інших неправомірних дій.
- **Конфіденційність** - забезпечення захисту конфіденційності інформації, яка є власністю держави або юридичної особи, або є особистою інформацією фізичної особи.
- **Цілісність** - забезпечення захисту інформації від несанкціонованих змін.
- **Доступність** - забезпечення можливості доступу до інформації уповноваженими особами.

Реалізація законодавчих вимог і регулювання інформаційної безпеки здійснюється **органами державної влади, органами місцевого самоврядування, підприємствами, установами, організаціями та громадянами**.

Організація забезпечення інформаційної безпеки в Україні передбачає:

- Розробку і впровадження нормативно-правових актів у сфері інформаційної безпеки.
- Створення та розвиток системи захисту інформації.
- Проведення заходів з підвищення рівня обізнаності населення про інформаційну безпеку.

Заходи захисту інформації

Для захисту інформації від несанкціонованого доступу, використання, модифікації, знищення, блокування, копіювання, поширення та інших неправомірних дій застосовуються такі заходи:

- Технічні заходи - це заходи, що забезпечують захист інформації за допомогою технічних засобів, таких як антивірусні програми, системи захисту від несанкціонованого доступу, системи резервного копіювання тощо.
- Організаційні заходи - це заходи, що забезпечують захист інформації за допомогою організаційних методів, таких як навчання персоналу основам інформаційної безпеки, розробка та впровадження політики інформаційної безпеки тощо.
- Правові заходи - це заходи, що забезпечують захист інформації за допомогою правових норм, таких як кримінальне та цивільне законодавство, законодавство про захист персональних даних тощо.

Джерела

- Інформаційна безпека
- Common Criteria