Загрози безпеці інформації в автоматизованих системах

Автоматизована система (**АС**) (англ. automated system) — сукупність керованого об'єкта й автоматичних керуючих пристроїв, у якій частину функцій керування виконує людина. АС являє собою організаційно-технічну систему, що забезпечує вироблення рішень на основі автоматизації інформаційних процесів у різних сферах діяльності (управління, проектування, виробництво тощо) або їх поєднаннях.

Це загальне визначення. У залежності від галузі застосування даються уточнені формулювання поняття «автоматизована система».

Автоматизовані інформаційні системи

Для автоматизованих систем, що використовуються в управлінні, дослідженнях, проектуванні та ін., зміст яких полягає в обробці інформації дано таке визначення (ДСТУ 2941-94):

Автоматизована система (у інформаційних технологіях) — система, що реалізує інформаційну технологію виконання встановлених функцій за допомогою персоналу і комплексу засобів автоматизації[4].

У цьому випадку автоматизовані системи розглядаються як інформаційні системи. Загалом АС — це система, яка складається з персоналу і комплексу засобів автоматизації його діяльності та реалізує інформаційну технологію виконання установлених функцій.

Залежно від виду діяльності розрізняють такі різновиди АС:

- АСК (автоматизовані системи керування), які у свою чергу в залежності від виду об'єкту керування поділяються на:
  - АСК технологічними процесами (АСК ТП);
  - АСК підприємствами (АСКП), виробництвом (АСКВ) тощо;
- Системи автоматизованого проектування:
  - САПР (системи автоматизованого проектування і розрахунку);
  - САПР ТП (системи автоматизованого проектування технологічних процесів) тощо;
- АСНД (автоматизовані системи наукових досліджень);
- АС оброблення та передавання інформації:
  - АІПС (автоматизована інформаційно-пошукова система);
  - АСІТО (автоматизована система інформаційно-термінологічного обслуговування) тощо;
- АСТПВ (АС технологічної підготовки виробництва);
- автоматизовані системи контролю та випробувань;
- АС, що поєднують функції, перелічених вище систем.

АС реалізують інформаційну технологію у вигляді певної послідовності інформаційно пов'язаних функцій, завдань або процедур, що виконуються в автоматизованому (інтерактивному) або автоматичному режимах.

Загрози безпеці інформації в автоматизованих системах

Під загрозою безпеки інформації розуміють події або дії, які можуть призвести до спотворення несанкціонованого використання або навіть до руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних засобів. З поняттям загрози безпеці тісно пов'язане поняття вразливості комп'ютерної системи (мережі).

Вразливість ІС - це можливість виникнення на якому-небудь етапі життєвого циклу автоматизованої системи такого її стану, за якого створюються умови для реалізації загроз безпеці інформації

Загрози безпеці інформації в автоматизованих системах (АС) - це будь-які події або дії, які можуть призвести до порушення цілісності, конфіденційності або доступності інформації, що обробляється в АС.

Загрози безпеці інформації в АС можна класифікувати за такими ознаками:

- За джерелом виникнення:
  - Природні (наприклад, стихійні лиха, пожежі, аварії);
  - Техногенні (наприклад, збої в роботі обладнання, помилки в програмному забезпеченні);
  - Людські (наприклад, злочинні дії, помилки персоналу).
- За характером дії:
  - Фізичні (наприклад, знищення або пошкодження носіїв інформації, обладнання);
  - Логічні (наприклад, несанкціонований доступ до інформації, її модифікація, блокування).
- За цілями:
  - Зловмисні (наприклад, крадіжка інформації, саботаж);
  - Ненавмисні (наприклад, помилки в роботі обладнання, людські помилки).

Людину, що намагається порушити роботу інформаційної системи або отримати несанкціонований доступ до інформації називають зломщиком, комп'ютерним піратом, хакером.

Хакер або гакер (англ. hacker, від to hack — рубати) — особа, що намагається отримати несанкціонований доступ до комп'ютерних систем, як правило з метою отримання секретної інформації. Також на слензі вживається у значенні — досвідчений комп'ютерний програміст або користувач.

Основні загрози безпеці інформації в АС належать

Несанкціонований доступ до інформації. Це найпоширеніша загроза, яка може призвести до крадіжки, модифікації або знищення інформації. Несанкціонований доступ може бути здійснений за допомогою різних методів, таких як:

- Зловживання правами доступу;
- Зловживання програмним забезпеченням;
- Зловживання фізичною доступністю до інформації;

- Зловживання мережевими з'єднаннями.

Знищення або пошкодження інформації. Ця загроза може бути реалізована шляхом фізичного знищення носіїв інформації, програмного забезпечення або обладнання, а також шляхом логічного знищення інформації, наприклад, шляхом її модифікації або блокування.

Викрадення інформації. Ця загроза може бути реалізована шляхом незаконного вилучення носіїв інформації, програмного забезпечення або обладнання, а також шляхом незаконного копіювання інформації.

Саботаж. Ця загроза може бути реалізована шляхом незаконного втручання в роботу обладнання або програмного забезпечення з метою порушення нормального функціонування АС.

Заходи безпеки інформації в АС

Для захисту інформації в АС застосовуються різні заходи безпеки, такі як:

- Фізичні заходи безпеки, які спрямовані на захист інформації від фізичних впливів, таких як знищення, пошкодження або викрадення. До таких заходів належать:
  - Контроль доступу до приміщення, де розташована АС;
  - Захист носіїв інформації від несанкціонованого доступу;
  - Захист обладнання від несанкціонованого доступу і впливу зовнішніх факторів.
- Логічні заходи безпеки, які спрямовані на захист інформації від логічних впливів, таких як несанкціонований доступ, модифікація або знищення. До таких заходів належать:
  - Аутентифікація і авторизація користувачів;
  - Контроль доступу до інформації;
  - Шифрування інформації;
  - Антивірусне програмне забезпечення.
- Організаційні заходи безпеки, які спрямовані на підвищення обізнаності персоналу про ризики безпеці інформації і формування культури безпеки в організації. До таких заходів належать:
  - Проведення інформаційних заходів з безпеки інформації;
  - Розробка і впровадження політики безпеки інформації;
  - Навчання персоналу основам безпеки інформації.

Заходи безпеки повинні розроблятися з урахуванням конкретних потреб організації і загроз, яким схильна інформація, що обробляється в АС.

Для оцінки ефективності заходів безпеки в організації проводиться аудит безпеки інформації. Аудит безпеки дозволяє виявити наявні уразливості і визначити заходи, необхідні для їх усунення.

Джерела

- Автоматизована система
- Хакер
- Голев Д.В., Кільдишев В.Й., Кононович В.Г. Інформаційна безпека інформаційно-

комунікаційних систем. Лабораторний практикум Частина 1 – Комплекси засобів захисту інформації від НСД: Навч. посібник / За ред. чл.-кор. МАЗ В.Г. Кононовича.– Одеса: ОНАЗ ім. О.С. Попова, 2010. – С.176