

Іванова С.М., к.пед.н., ст. дослідник,
Інститут цифровізації освіти
Національної академії педагогічних
наук України, Київ

ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Вступ. Сьогодні інформація стала одним із найцінніших ресурсів сучасного суспільства. З розвитком інформаційно-комунікаційних технологій (далі – ІКТ) спостерігається стрімке зростання обсягу даних, які генеруються, передаються і зберігаються в інформаційних системах. Проте з цими перевагами виникають нові виклики, пов’язані із захистом інформації від різноманітних загроз, таких як кіберзлочинність, витоки даних і атаки на інформаційні системи. Розглянемо основні аспекти захисту інформації в ІКТ, методи, засоби, а також законодавчі та етичні аспекти.

Зі зростанням цифровізації та інтеграції технологій у всі сфери життя, захист інформації стає важливим і актуальним [1]. На прикладі великих компаній та державних установ ми можемо спостерігати численні випадки кіберінцидентів, які призводять до фінансових втрат, втрати довіри з боку користувачів і репутаційних збитків. За даними різних досліджень, витрати на кібербезпеку зростають щорічно, проте численність атак не зменшується.

Основні загрози інформації. Кібератаки можуть бути різного характеру, і серед них можна виділити такі основні типи:

1. *Малваре (malware)* – шкідливе програмне забезпечення (далі – ПЗ), яке викрадає дані, шифрує їх або завдає шкоди системам;
2. *Фішинг* – соціальна інженерія, яка використовується для отримання конфіденційної інформації користувача через підроблені сайти чи електронні листи;
3. *Атаки з відмовою в обслуговуванні (DoS)* – спрямовані на блокування доступу до системи шляхом перевантаження її запитами;
4. *Експлуатація вразливостей* – використання вразливості ПЗ для отримання несанкціонованого доступу до системи;
5. *Витоки даних* – ненавмисне або навмисне розголошення конфіденційної інформації.

Методології захисту.

1. *Проведення оцінки ризиків.* Оцінка ризиків є критично важливим етапом у процесі забезпечення інформаційної безпеки. Вона включає в себе визначення цінності інформації, вразливостей системи та потенційних загроз. На основі отриманих даних можна розробити відповідні заходи для захисту.

2. *Використання технічних засобів захисту.* Основні технічні засоби, які забезпечують інформаційну безпеку:

- Антивірусні програми – для виявлення і знешкодження шкідливого ПЗ.
- Фаєрволи – для контролю вхідного і вихідного трафіку та блокування небезпечних запитів.
- Шифрування – захист даних під час їх передачі або зберігання, щоб запобігти несанкціонованому доступу.
- Системи виявлення вторгнень (IDS) – для моніторингу і аналізу активності в системі.

3. *Організаційні заходи.* Організаційні заходи включають створення політик безпеки, проведення навчання співробітників і розробку планів реагування на інциденти. Це дозволяє забезпечити не лише технічний, а й людський аспект безпеки.

4. *Юридичні та етичні аспекти.* Захист інформації також пов'язаний з нормативно-правовим регулюванням. В Україні існують закони, які регулюють конфіденційність даних, наприклад, Закон України «Про захист інформації в інформаційно-комунікаційних системах» [1]. Крім того, гнучкість етичних стандартів у сфері ІКТ є важливим аспектом, оскільки зловживання інформацією може призвести до серйозних наслідків.

Висновки. Захист інформації в інформаційно-комунікаційних системах є складним та багатогранним процесом, що вимагає комплексного підходу. Сучасні загрози вимагають не лише використання високотехнологічних рішень, але й врахування людського фактору, організації процесів, а також дотримання юридичних і етичних стандартів. Тільки за умови системного підходу до даної проблеми можливо забезпечити надійний захист інформації та зберегти конфіденційність даних у світі, де цифрові загрози постійно еволюціонують. З огляду на зростаючу важливість інформаційної безпеки, можна стверджувати, що ця тема залишатиметься в центрі уваги як фахівців з ІТ, так і законодавців, оскільки атакуючі технології

постійно вдосконалюються, а інформація продовжує залишатися у вищій ціннісній категорії.

Список використаних джерел

1. Закон України «Про захист інформації в інформаційно-комунікаційних системах». № 1089-IX від 16.12.2020}. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>.