Основи інформаційної безпеки: захист від кібератак, криптографія, безпека даних

Владислав Коляденко,
студент кафедри комп'ютерних наук, КН-24,
ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна,
e-mail: KoliadenkoVV@krok.edu.ua
Віра Ткаченко,
к.ф.-м.н., доцент, доцент кафедри інформаційного менеджменту,
математики та статистики,
ВНЗ «Університет економіки та права «КРОК», м. Київ, Україна,
e-mail: tkachenkov@krok.edu.ua,
ORCID: 0000-0001-6064-5474

На сьогоднішній день, враховуючи сучасні обставини та стрімкий розвиток технологій, інформаційна безпека є надзвичайно важливою навичкою для користувачів різних пристроїв та мережі Інтернет, адже мережі, комп'ютерні системи та цифрові ресурси використовуються у всіх сферах діяльності, від бізнесу та освіти до урядових структур і медицини. Кібератаки, викрадення даних, порушення конфіденційності та інші види злочинної діяльності в Інтернеті можуть призвести до серйозних наслідків. Саме тому основи інформаційної безпеки, зокрема захист від кібератак, криптографія та забезпечення безпеки даних, є критично важливими для підтримки безпеки та довіри у цифровому середовищі.

Аби мати впевненість у перемозі, треба знати свого ворога. Небезпека потребує роз'яснень: кібератаки можуть мати різні форми – від шкідливих програм до більш складних атак, що спрямовані на порушення цілісності або конфіденційності даних. Однією з найбільших загроз є DDoS-атаки, які направлені на перевантаження системи та її виведення з ладу, що може призвести до зупинки веб-сайтів чи сервісів. Іншою поширеною загрозою є фішинг (англ. fishing), коли злочинці використовують підроблені веб-сайти або електронні листи для того, щоб вкрасти особисті дані користувачів. Для захисту від таких атак важливо впроваджувати мережеві фільтри, системи виявлення вторгнень (IDS), системи запобігання вторгнень (IPS), а також постійно оновлювати програмне забезпечення та використовувати брандмауери для обмеження доступу до важливих систем і ліцензовані антивірусні програми, які допоможуть вам із знешкодженням особливо небезпечних загроз. Захист від DDoS-атак може включати використання спеціалізованих сервісів для розподілу навантаження, а також систем для фільтрації підозрілих запитів на рівні серверів.

Важливий не тільки захист під час самих атак, а і ті методи, які можна застосовувати на регулярній і постійній основі, наприклад методи із криптографії. Криптографія – це наука та практика надсилання безпечних зашифрованих повідомлень (даних) між двома або більше сторонами [1]. Існує два основні типи шифрування: симетричне і асиметричне.

Симетричне шифрування використовує один і той самий ключ для

шифрування і дешифрування даних [2]. Однак основною проблемою цього методу є необхідність безпечної передачі ключа між сторонами.

Асиметричне шифрування, або шифрування з відкритим ключем, використовує два ключі: один для шифрування (відкритий ключ) і інший для дешифрування (закритий ключ) [2]. Цей метод є більш безпечним для обміну даними через відкриті канали зв'язку, оскільки закритий ключ не передається.

Крім шифрування, важливим інструментом криптографії є хешування, яке використовується для перевірки цілісності даних. Хеш-функція перетворює повідомлення або файл у короткий, фіксований за розміром рядок (хеш), що дозволяє перевірити, чи не були дані змінені. Хешування є важливим елементом багатьох криптографічних протоколів, таких як цифрові підписи, що забезпечують автентичність електронних документів. Цифровий підпис, створений за допомогою асиметричного шифрування, дозволяє підтвердити, що повідомлення або документ дійсно походить від зазначеного відправника і що їх зміст не був змінений після підписання [3].

Крім того, в рамках інформаційної безпеки, особливу увагу варто приділяти захисту даних на всіх етапах їх зберігання та передачі. Для цього використовуються різноманітні методи, такі як шифрування дисків і файлів, а також контроль доступу до інформаційних систем і баз даних. Застосування двох факторної аутентифікації, коли для доступу до системи потрібно пройти кілька етапів перевірки (наприклад, пароль та одноразовий код, надісланий на мобільний телефон), також значно підвищує рівень безпеки. Безпека даних включає також питання управління доступом і правами користувачів. Важливо впроваджувати політики мінімальних прав, що обмежують доступ до інформації тільки тими користувачами, які мають необхідні дозволи для виконання конкретних завдань. Крім того, необхідно регулярно проводити аудит доступів і перевіряти ефективність запроваджених заходів безпеки.

Але навіть незважаючи на досягнення в галузі інформаційної безпеки, нові загрози постійно еволюціонують, тому важливо не лише впроваджувати сучасні технології захисту, а й розвивати стратегії, що дозволяють адаптуватися до нових викликів. Це вимагає постійного вдосконалення знань та навичок у сфері інформаційної безпеки, оновлення інструментів захисту, а також постійного моніторингу безпеки інформаційних систем.

Таким чином, можна стверджувати, що забезпечення належного рівня інформаційної безпеки є необхідною умовою для стабільної і безпечної роботи як окремих осіб, так і організацій, які функціонують в умовах сучасної цифрової економіки. Кібератаки, криптографія та захист даних є основними елементами цієї складної системи, що повинна охоплювати всі аспекти збереження, обробки та передачі інформації. Зважаючи на постійно зростаючі ризики та загрози, важливою є не лише впровадження ефективних технологічних рішень, а й створення культури безпеки в організаціях, що передбачає усвідомлену і відповідальну поведінку всіх учасників інформаційних процесів.

Ключові слова: КРИПТОГРАФІЯ, Симетричне шифрування, Асиметричне шифрування.

Список використаних джерел

1. Nick CryptoDiffer. Що таке криптографія? 2022. URL: https://tsecrypto.com/article/shho-take-kryptografiya/

2. Введення в криптографію: симетричне шифрування // MarkupUA – URL: https://markup-ua.com/vvedennya-v-kriptografiyu-simetrichne-shifruvannya/

3. Ткаченко В.С. Конспект лекцій з дисципліни «Прикладна криптологія» (частина 1). 102с. – Вінниця: ДонНУ, 2022