

ВИКОРИСТАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ ПРОГРАМУВАННЯ В ЗАДАЧАХ ЗАХИСТУ ІНФОРМАЦІЇ

У сучасній розробці бізнес - додатків, велику кількість часу приділяють питанням безпеки передачі, обробки та зберігання інформації в різних інформаційних системах. Це закономірне явище, оскільки веб - додатки вже давно є улюбленими мішенями зловмисників, так як можуть забезпечити доступ до цінної інформації.

Метою роботи є дослідження загроз витоку інформації в інформаційних системах та формування рекомендацій щодо практичного застосування сучасних технологій програмування при вирішенні питань захисту інформації.

В першу чергу авторами роботи звертається увага на проблему написання безпечного коду. Найчастіше при роботі з буферами даних розробники програмного забезпечення забувають очищати пам'ять, що призводить до винятків і зупинки роботи програми.

Хорошим тоном безпечного коду є обробка виключень в блоках try - catch, застосування принципу інкапсуляції, дотримання стандартів оформлення, а також тестування.

Тестування є обов'язковим інструментом розробника, так як дозволяє виявити безліч помилок ще на стадії розробки програми.

Слід окремо звернути увагу на стратегію роботи з паролями користувача. Найчастіше вони зберігаються в базу даних в явному вигляді, що при успішній sql - ін'єкції може привести до їх витоку. Для уникнення такої ситуації пропонується використовувати алгоритми хеш - функцій для перетворення пароля в неявний вид.

Одна з найбільш поширених загроз витоку інформації - є витік по каналу зв'язку. Їм може виступати ТСП - з'єднання з сервером. За допомогою сніффінга зловмисник перехоплює і отримує доступ до даних, які передаються в перебігу обробки з'єднання. Для виключення такої ситуації розробникам програмного забезпечення рекомендується використовувати шифрування інформації на базі доступних алгоритмів, наприклад "Калина". Таким чином, якщо відбувається несанкціонований доступ до інформації за допомогою перехоплення трафіку - шкідник не зможе з ними нічого зробити, тому що вони зашифровані.