Комплексна система захисту інформації (КСЗІ)

м.н.с Ганна Гришанова

Вимоги до захисту інформації веб-сторінки від несанкціонованого доступу

Актуалізацію розміщених на веб-сторінці інформаційних ресурсів та керування доступом до них слід здійснювати за допомогою автоматизованої системи УкрІнтеі, в якій має бути створена КСЗІ, яка потребує виконання переліку вимог до такої АС.

Інформацію веб-сторінки поділяють на дві категорії: загальнодоступну та технологічну.

Загальнодоступну інформацію може використовувати будь-яка особа, що має доступ до Інтернету.

Технологічна інформація стосується адміністрування та керування обчислювальною системою АС і засобами оброблення інформації. Це дані про мережні адреси, імена, персональні ідентифікатори та паролі користувачів, їх повноваження та права доступу до об’єктів, інформація журналів реєстрації дій користувачів, інша інформація: встановлені робочі парметри окремих засобів захисту, параметри функціонального ПЗ тощо. Технологічну інформацію можуть використовувати лише вповноважені користувачі - співробітники служби зхахисту інформації й персонал, що забезпечє функціонування АС. Слід звернути увагу на те, що розміщувати на веб-сторінці конфівденційну інформацію чинне законодавство не дозволяє. Якщо інформація не є власністю держави або інфоормацією з обмеженим доступом, вимогу щодо захисту якої встановлено законом, то власник інформації може запроваджувати правила доступу до неї на свій розсуд, щоправда, захист конфіденційності такої інформації в Інтернеті гарантувати не можна.

Розташування веб-сторінки

Веб-сторінка може бути розміщеною як на території власника інформації, так і на території сторонньої організації. В останньому випадку заходів із захисту інформації слід вживати не лише власникам інформації, але й власникам автоматизованої системи, де розміщено веб-сторінку. Власник інформації, виходячи з чинного законодавства, визначає правила доступу до неї, а власник системи здійснює захист інформації, зокрема забезпечує відповідне розмежування доступу до такої інформації.

Доступ до технологічної інформації

Доступ до технологічної інформації та передавання даних для актуалізації загальнодоступної інформації здійснюють у два способи: з робочої станції, розташованої на тій самій території, що і веб-сервер (установи-власника веб-сторіки або оператора), чи з терміналу веб-сервера (технологія Т2). Технологія Т1 відрізняється від технології Т2 наявністю у другому випадку незахищеного середовища, яке не контролюється, і додатковими вимогами щодо ідентифікації та автентифікації між КЗЗ робочої станції і КЗЗ веб-сервера під час спроби розпочати обмін інформацією та забезпечення цілісності інформації під час обміну.

Стандартні функціональні профілі захищеності

НД ТЗІ 2.5-010-03 визначає такі профілі захищеності оброблюваної інформації:

За умови, що доступ до технологічної інформації та передавання даних для актуалізації загальнодоступної інформації здійснюється за технологією Т1:

“КА-2, ЦА-1, ЦО-1, ДВ-1, ДР-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1”.

За умови, що доступ до технологічної інформації та передавання даних для актуалізації загальнодоступної інформації здійснюється за технологією Т2:

“ КА-2, КВ-1,ЦА-1, ЦВ-1, ЦО-1, ДВ-1, ДР-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1, НВ-1”.

Мінімальний рівень гарантій

Мінімальним достатнім рівнем гарантій реалізації КЗЗ веб-сторінки є рівень Г-2.

Загрози безпеці інформації у мережах

Розподіл ресурсів та інформації у просторі робить можливою наявність мережних атак. Під віддаленою атакою розуміють атаку на розподілену обчислювальну систему, що здійснюють програмні засоби каналами зв’язку. Така атака може бути здійснена на протоколи і мережні служби, а також на операційні системи та прикладні програми вузлів мережі.

Типові вразливості розподілених систем відповідно до “IT Baseline Protection Manual - BSI (Federal Agency for Security in Information Technology” (October 2000):

- угадування паролів, або атаки за словником;
- реєстрація та маніпуляції з мережним трафіком;
- імпорт фальшивих пакетів даних;
- експлуатація відомих уразливостей програмного забезпечення (мови макросів, помиллки в ОС, служби віддаленого доступу тощо).
-

Причини вразливостей мережних систем

- використання спільного середовища передавання (наприклад, Ethernet, радіоканал);
- застосування нестійких алгоритмів ідентифікації віддалених об’єктів;
- використання протоколів динамічної (адаптивної) маршрутизації;
- застосування алгоритмів віддаленого пошуку.

Безпека взаємодії відкритих систем

Зараз частково розроблено стандарти (робота над їх створенням триває), спрямовані на забезпечення захисту інформації у відкритих системах, і відповідні механізми захисту.

Література

ISO/IEC 7498-2:1989;

НД ТЗІ 2.5-010-03;

М.В. Грайворонський, О.М.Новіков. Безпека інформаційних систем.