49. Сигурност на информационни системи – функционални и архитектурни решения

Информационна сигурност се нарича практиката на защита на информацията от неправомерен достъп, използване, разкриване, увреждане, промяна, преглед, запис или разрушаване. В контекста на информационните системи това е централно понятие с голяма важност. Необходимо е системата да притежава пет базови услуги за сигурност: конфиденциалност на данните, управление на достъпа, автентикация, цялостност на данните, non-repudiation (невъзможност за отричане от получени/изпратени данни). Мерките за осигуряване на информационна сигурност чрез тези услуги могат да бъдат административни, технически и физически.

Административните (организационни, процедурни) мерки включват одобрени политики, процедури, стандарти и указания. Те информират служителите какво трябва и какво не трябва да правят при всекидневната си работа. Пример за такива мерки са политиките за сигурност, план за действие в аварийни ситуации. Тези мерки формират базата за техническите и физическите мерки. При системата за електронно гласуване примерна административна мярка е допускането до упражняване на глас само на граждаждани на съответната страна, които по закон имат това право. Всички останали потребители или не би трябвало да имат достъп до системата или би трябвало да имат ограничен достъп, който да не им позволи да използват пълната функционалност на системата.

Техническите мерки представляват използването на софтуер, мониторинг и контрол на достъп до информацията и компютърните системи. Примери за това са пароли, антивирусен софтуер, защитни стени, контроли за достъп (кой до коя папка/файл има достъп), криптиране и други. Важен логически контрол са ограничените права при използване на компютърна система. Чрез ограничаване на правата на всеки потребител, програма или системен процес се предоставят само необходимите права за изпълнение на определените задачи.

Физически мерки са мониторинга и контрола над работната среда. Контрол на достъпа, видео наблюдение са пример за подобен тип мерки. Важен аспект от защитата на информацията при обработката и съхранението ѝ в компютърни системи и предаването ѝ в локални мрежи е физическата защита на кабелната система, комуникационното оборудване, сървърите и работните станции от неоторизиран достъп.