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. За осигуряването ѝ съществуват различни механизми: шифриране, механизми за управление на достъпа, механизми за осигуряване цялостта на данните, автентикация, механизми за запълване на трафика, механизми на нотаризация, механизми за управление на маршрутизацията.

Шифрирането е процес на преобразуване на данните за обезпечаване тяхната конфиденциалност. Шифрирането осигурява използване на криптографско преобразуване с цел да се направят данните невъзможни за четене или осмисляне. Шифрирането се реализира заедно с обратната функция – дешифриране. При използване на механизма шифриране е от особена важност генерирането, съхранението и разпространението на криптографските ключове. Шифрирането се използва основно за осигуряване на услугата конфиденциалност, но може да поддържа и други услуги – автентификация, цялостност, управление на достъпа.

Механизмите за управление на достъпа се използват за осигуряване на услуги, реализиращи политиката за управление на достъпа. При управление на достъпа се използват следните средства: бази данни, в които се намират списъци за управление на достъпа; пароли или друга информация за идентификация; удостоверения, които гарантират правата на достъп; маркери на сигурност, асоциирани със субектите и обектите на достъп; време на искания достъп; маршрут на искания достъп; продължителност на искания достъп и друга информация.

Съществуват два типа механизми за осигуряване цялостността на данните - за защита цялостта на отделен пакет данни и за защита цялостта на последователност от пакети данни.

В най-общ случай под автентификация се разбира установяването истинността на съобщения, източник на данни, приемник на данни. Механизмите за автентификация, които са известни като протоколи за автентификация, са обект на различни стандарти.

Механизмите за запълване на трафика се използват за осигуряване на конфиденциалност на трафика. Включват генериране на случайни числа, запълване на пакетите с допълнителна информация, предаване на пакетите в лъжливи направление, запълване на постоянна дължина на пакетите. Механизмите за запълване на трафика са ефективни само когато се използват в съчетание със средства за осигуряване на конфиденциалност. При самостоятелно използване е виден фиктивния характер на допълнителната информация.

Механизмите за нотаризация използват трета страна, ползваща се с доверието на двата субекта. Третата страна потвърждава комуникационните характеристики (цялостност, време, личност на източника и получателя) на предаваните данни.

Механизмите за управление на маршрутизацията решават следните задачи: осигуряване на конфиденциалност, избор само на надеждни физически канали и мрежови устройства при предаване на данни, забрана за предаване на данни по ненадеждни канали, избор на алтернативни пътища при откриване на атаки.