ПРОГРАМ РАДА
ISS/KS I224

Идентификација, картице, финансијске услуге и технике безбедности у ИТ

Овај програм рада усвојен је на седници Комисије која је одржана 18.05.2013. године, а одобрен је од стране Стручног савета за стандардизацију у областима електротехнике, информационих технологија и телекомуникација, на седници која је одржана 18.09.2013. године.

0 Увод

Област рада Комисије за стандарде KS I224 јесте стандардизација у области личне идентификације, картица и електронских потписа за примене у банкарству, телекомуникацијама, транспорту, електронској управи и електронском пословању и примене техника сигурности у информационој технологији. Комисија под тим називом није никада постојала, али се облашћу картица бавила Комисија KS I068, *Банкарство и сродне финансијске делатности*, а облашћу техника сигурности у ИТ комисија KS I1/27, *Технике сигурности у информационој технологији* која је првобитно основана 1996. године, обновљена 1998. године и поново обновљена 2010. године.

Комисија KS I224 прати рад следећих комитета и поткомитета:
- CEN/TC 224, *Лична идентификација, електронски потпис и картице и њима припадајући системи и операције;*
- ISO/IEC JTC 1/SC 17, *Картице и лична идентификација,*
- ISO/IEC JTC 1/SC 27, *Технике сигурности у информационој технологији*, и
- ISO/TC 68, *Финансијске услуге*.

1 Пословно окружење

1.1 Опште

Са порастом трговине растао је и обим финансијског пословања, како у националним тако и у светским оквирима. Због тога је било потребно увести нове видове финансијских трансакција и услуга преношења средстава, па су временом настајале платне картице (кредитне и дебитне). Са развојем туризма и путничког саобраћаја, са интензивним кретањем људи, све више на обиму добијале су финансијске трансакције са мањим износима у виду појединачних плаћања услуга и производа, па посредник у финансијским операцијама више нису биле само банке. У широку употребу уведени су појмови „електронско пословање“, „електронска трговина“, „електронско плаћање“ и др.

Зато се 1988. године указала потреба за формирањем Комисије KS I068 како би се усвојили сви неопходни стандарди, како из области финансијских трансакција, тако и из области банкарских картица. У каснијем периоду, употреба картица се проширила на идентификационе картице (картице за евиденцију запослених, за студенте), затим на нову генерацију биометријских путних докумената, дозвола за управљање моторним возилима и сродним документима.

Информације су увек представљале важну имовину сваке организације, без обзира на то у ком облику се размењују или чувају. Успостављањем информационих система број информација се ширио. Неправилно

поступање са њима, њихово откривање или губитак проузрокују негативне ефекте на пословање и углед организације. Незаштићени информациони системи су подложни различитим врстама претњи, интерним или екстерним, случајним или злонамерним, као што су рачунарски потпомогнуте преваре, саботаже и вируси. Повреда информационе безбедности увек може довести до неовлашћеног приступа, крађе, оштећења или губитка значајних информација. Зато је било важно успоставити поступке безбедности у циљу заштите информација и свих комуникација којима се преносе информације. Безбедност информација је све до седамдесетих година 20. века била ограничена на одређене области примене, као што су банкарство и финансијско пословање и електронска управа (е-влада).

Са појавом Интернета и електронског пословања безбедност је добила приоритет у информационим и комуникационим технологијама, а постала је и предмет законодавства. Нпр. организације које развијају електронске сервисе на даљину (е-пословање, е-управа) морају да осигурају: контролу приступа апликацијама, дозволе само одређеним корисницима, корисничку идентификацију, ауторизацију. Електронски потписи обезбеђују интегритет података и то помаже убрзању раста безбедног електронског пословања и тиме елиминисању папирних трансакција. Истовремено, корисницима је потребно поверење у ефективност имплементиране безбедности.

Из тих разлога се на нивоу Здруженог техничког комитета ISO/IEC JTC 1 указала потреба за оснивањем Поткомитета SC 27 под називом *Технике сигурности у информационој технологији*. По посебној убрзаној процедури усвојен је стандард ISO/IEC 17799 који је припремио Британски институт за стандардизацију (у форми BS 7799), сада пренумерисан у ISO/IEC 27002 у серији стандарда 27000. Тада је донет и стандард ISO/IEC 27001 (систем менаџмента безбедношћу информација - ISMS), при чему се водило рачуна да се подржи конзистентна и интегрисана имплементација и примена са сродним стандардима менаџмента: ISO 9001 (квалитет), ISO 14001 (заштита животне средине) и ISO 22000 (безбедност хране).

Због тога се и у Србији указала потреба за формирањем комисије KS I1/27 како би се усвајали сви неопходни стандарди из серије стандарда 27000.

С обзиром на тенденције развоја и примене ових стандарда, очекује се све већи број њихових корисника. Стога ће од посебног значаја бити сарадња са малим и средњим предузећима (МСП), како са предузећима која се баве консалтингом и услугама имплементације ISMS-а, тако и са предузећима из области ICT-а у која је потребно увести ISMS ради безбедности њиховог пословања. Сарадња треба да буде и са оним предузећима која се баве израдом картица. МСП из области ICT имају потребу да прате стандарде који се односе на: физичке карактеристике свих врста картица (папирних, пластичних, „смарт“ и RFID), персонализацију картица и перформансе читача картица.

1.2 Захтеви тржишта

Технологија магнетне траке је већ дуго у употреби и још увек напредује. Најзначајнији корисници стандарда из ове области су наручиоци картица: банке, трговине, државни органи, превозници и други, као и предузећа која се баве израдом картица. Најкритичнији захтеви у овом тренутку су у вези са идентитетом и питањима управљања идентитетом са којим се суочавају све власти у свету.

Напредак технологије и повећање нивоа знања о рачунарима довели су до све већих захтева у погледу безбедности, пре свега финансијских трансакција. Како се повећавала потреба за увођењем информационих система, а данас их скоро свако предузеће има, расла је и потреба за безбедношћу информација и информационе имовине, што је могуће увођењем ISMS-а. Највећи корисници стандарда су предузећа која су увела ISMS или имају намеру да то учине, као и предузећа која пружају консултантске услуге у увођењу и одржавању ISMS-а. У скорије време је доста оних који се баве обуком из те области. Стога се ти стандарди широко примењују на националном нивоу.

1.3 Технолошки трендови

Некадашње платне картице се полако замењују мултифункционалним (чип) картицама. Технологија чип-картица пружа могућност да се више апликација налази на једном чипу. Поред могућности да се изврше финансијске трансакције моћи ће да се користи и као картица за превоз, за складиштење разних података итд. Сваки податак који може да се дигитализује, може и да се стави на чип, тако да је могуће да картица постане и специфична „мини-база података“. Сваку функцију картице која више није потребна могуће је избрисати, а неке нове додавати.

Доступност личних података олакшава могућност преваре. Међутим, чип-картица смањује могућност злоупотреба, јер се њоме уводи утврђивање аутентичности.

У свету, корисници све више траже заштиту приватности својих информација и података. Безбедност и приватност информационих технологија су јако сличне и комплексне. То се нарочито може видети у области менаџмента идентитетом, нпр. ко управља личним подацима и ко је овлашћен да их користи. То је препознато на међународном нивоу као технолошки изазов, па је у Поткомитету SC 27 формирана нова радна група WG 5, *Менаџмент идентитетом и технологије приватности*, која већ доноси серију стандарда ISO/IEC 24760 (Оквир за менаџмент идентитетом) и ISO/IEC 29100 (Оквир приватности).

Стандардизоване технике безбедности постају обавезне у електронској трговини (e-commerce) и мобилној трговини (m-commerce), здравству, телекомуникацијама и у многим другим како комерцијалним секторима тако и у владином сектору. Технологије као што је радиофреквенцијска идентификација (RFID) поставиле су нове изазове у погледу безбедности и приватности и, с обзиром на посебне принуде, захтевају се одговарајућа решења, као што су криптографске технике, потврда веродостојности итд.

1.4 Тржишни трендови

Примена идентификационих картица свакодневно се проширује. Очекује се ускоро и увођење електронске здравствене књижице, тако да су заиста велике могућности примене картица на тржишту.

Организације све више препознају важност безбедности унутар система и процеса софтверског инжењерства, као и унутар ланца снабдевања. Такође, постоје потребе за стандардима који упућују на менаџмент инцидентима, на специфичне активности у руковању могућим дигиталним доказима и на процесе заједничких истраживања кроз различите сценарије истраживања. Актуелни су и стандарди који се баве безбедношћу мрежа, сајбер-безбедношћу, анализом рањивости софтвера.

1.5 Еколошко окружење

Сама тенденција коришћења електронских комуникација доводи до смањења потрошње папира. А што се тиче потрошње ресурса и енергије и загађења окружења и генерисања отпада, може се говорити само уопштено за све организације које користе информационе уређаје у свом раду. Циљ је безбедан рад уређаја и њихово адекватно одлагање по престанку рада.

1.6 Заинтересоване стране

Битно је у рад укључити све заинтересоване стране. На међународном нивоу поткомитети ISO/IEC JTC 1 / SC 17 и SC 27 тесно сарађују са поткомитетима и комитетима, посебно на изради стандарда из области биометрике, RFID, финансијских услуга, информатике у здравству, интелигентних транспортних система, рачунарских решења у тзв. "облаку" (cloud computing). Тако би у рад Комисије требало укључити и нове заинтересоване стране, посебно из тих области, као и чланове министарстава.

1.7 Укључивање малих и средњих предузећа (МСП)

Мала и средња предузећа углавном потпадају под велике произвођаче картица. Међутим, нека од ових малих и средњих предузећа специјализована су у својој области деловања и тако постоје релативно независно од шире организације која стоји иза њих. Поред тога још увек постоји известан број независних малих и средњих предузећа, тако да је неопходно подстицати укључивање малих и средњих предузећа на националном нивоу. Било би препоручљиво у рад Комисије укључити МСП која се баве услугама „cloud computing“, криптографске технике и пројектовањем система.

2 Циљеви и стратегија

Циљеви Комисије су следећи:
– преузимање преосталих европских стандарда из области идентификације и картица,
– преузимање преосталих стандарда из серије 27000,
– редовно преиспитивање стандарда и њихова замена новим издањима.

Потребно је пратити трендове који постоје у земљи и доносити годишње планове са потребним стандардима. Потребно је у што већем броју превести стандарде на српски језик, анимирањем чланова Комисије.

3 План активности

Једна од главних активности Комисије за наредни период јесте преузимање стандарда који се односе на захтеве за безбедност идентификације, утврђивања аутентичности и електронског потписа (IAS), који су неопходни за електронску управу и електронско пословање. Такође и превођење на српски језик најновијег издања стандарда ISO/IEC 27000, с обзиром на то да се ради о речнику који треба да представља окосницу терминологије ове серије стандарда.

4 Корисни линкови за све наведене активности

Све додатне информације о објављеним, повученим и анотираним стандардима Комисије KS I224 могу се погледати на следећој интернет-адреси: сви стандарди комисије I224, а о планираним пројектима за наредни период на интернет-адреси: планирани пројекти комисије I224.

Све додатне информације о међународним комитетима и европском комитету чији рад прати Комисија, о њиховој области рада, земљама чланицама, структури, објављеним стандардима и планираним пројектима могу се погледати на следећим интернет-адресама:

CEN/TC 224

ISO/IEC JTC 1 / SC 17

ISO/IEC JTC 1 / SC 27

ISO/TC 068