

JRMAD METODO PANAUDOJIMAS TAIKANT INFORMACINIŲ TECHNOLOGIJŲ SAUGOS POLITIKĄ

Eglė Švedaitė

Vilniaus Gedimino technikos universitetas
El. paštas: egle@vgtu.lt

Santrauka. Nagrinėjama saugos lankstumo problematika veikiančiose informacinių technologijų sistemose. Ieškoma būdų užtikrinti saugos reakcijos laiko sklandų prieinamumą, kai projektai dar tik kuriami. Atlikta projektų apžvalga, susistemintos projekto kūrimo bei vystymo dalys. Išvados panaudotos surasti metodui, kuris paneigtų projekto dalių taisyklę ir būtų išeitis saugos planavimui projektų kūrimo pradžioje. Analizės rezultatas: JRMAD mišrusis metodas, leidžiantis vienu metu vykdyti abi projekto dalis ir tuo pačiu metu keisti sistemą.

Reikšminiai žodžiai: projektas, saugos problemos, IT projektas, JRMAD metodas, būtinasis saugumas.

Įvadas

Dar prieš dešimt metų *Projektų valdymas* buvo nauja ir sunkiai apčiuopiama sritis. Dabar informacinės sistemos jau kuriamos pagal atrastus ir išnagrinėtus metodus, aiškiai apibrėžiančius projekto etapus ir leidžiančius pasirinkti norimą rezultatą (laiką, kainą, kokybę). Akivaizdu, jog vienokios ar kitokios informacinės sistemos poreikis atsiranda čia ir dabar, todėl kalbėti apie ilgą ir detalai apgalvotą procesą tiesiog nėra prasmės. Juolab kad informacinių technologijų (toliau – IT) produktas ne visada yra aiškiai apibrėžtas ar žinomas iki vėlyvų produkto kūrimo etapų. Reikia paminėti, jog IT projekto fazės sudėtingesnės nei įprastų inžinerinių projektų, jos dažnai vyksta vienu metu arba net yra spiralės formos (Saulis *et al.* 2008). Atsižvelgiant į aibę specifikacijos reikalavimų kuriant produktą (ar jį valdančią sistemą) per pakankamai trumpą laiką, kurio dažniausiai reikalauja užsakovai, bei daugelį keitimų, kurie vyksta kūrimo etapu, saugumo klausimas, deja, yra vienas iš paskutiniųjų ir kuriamam produktui apgalvojamas paviršutiniškai be didesnių funkcinių reikalavimų. Šiandienos projekto užsakymo ir jo valdymo pavyzdys galėtų būti sistemos, valdančios nutolusius pardavimo taškus, sukūrimas: užsakovas iškelia pagrindinius koncepcinius būsimos sistemos reikalavimus, vykdytojas (IT darbus atliekanti kompanija) juos specifikuoja, įvykdo ir atiduoda produktą. Sistema sudėtinga, pagal koncepcinius reikalavimus turi užtikrinti bendrąjį (aptariama straipsnyje) saugumą.

Tokia sistema (produktas) yra funkcionali ir saugi, ji atiduodama užsakovui, ir projektas baigtas.

Straipsnyje nagrinėjama viena pagrindinių šiandienos sistemos administravimo problemų: saugumas yra papildomas keblumas, norint greitai ir efektyviai šalinti iškilusias problemas jau po projekto sukūrimo – sistemos / produkto veikimo metu. Dažnai ugniasienės, slaptažodžių kodavimas ar kitos įprastos saugumo priemonės yra nelankstaus ir, administraciniu požiūriu, nepatogaus darbo priežastis, ypač kalbant apie nutolusius sistemos taškus. Straipsnyje aptariamas darbo organizavimo principas (besivystantis į metodą), kurio naudojimas gali sumažinti reakcijos laiką ir efektyviai šalinti iškilusias problemas.

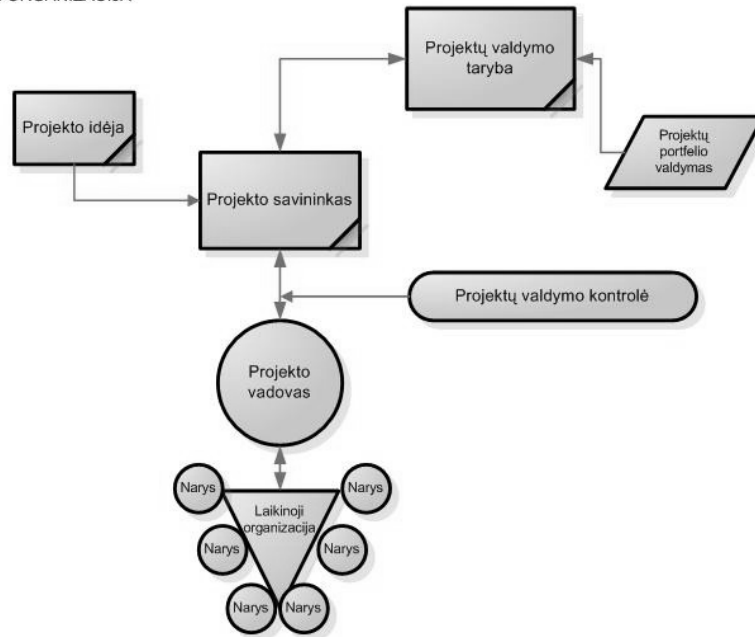
Bendrai apie projektus

Populiarėjant sąvokai *projektas* (projektų vadovas) ir naudojant ją ten, kur kalbama apie veiklą, dažnai iškraipoma pradinė projekto reikšmė ir jo funkcionalumo užduotis. *Projektas* yra laikina veikla, skirta unikalios produkto ar paslaugos sukūrimui (Būda *et al.* 2006). Projektai skirstomi į tipus pagal darbo metodų ir tikslų apibrėžimo sudėtingumą:

- I tipas – inžineriniai;
- II tipas – naujų gaminių ir paslaugų kūrimo;
- III tipas – sistemos kūrimo ir įdiegimo;
- IV tipas – tyrimo ir pokyčių.

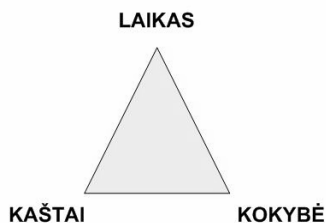
Projekto veiklą vykdo projektinė organizacija (žr. 1 pav.).

PROJEKTINĖ ORGANIZACIJA



1 pav. Organizacinė struktūra
Fig. 1. Organizational structure

Projekto strateginiai tikslai realizuojami pagal „Protingumo (angl. *Smart*) principus“. Tikslai: protingi (angl. *Smart*), pamatuojami (angl. *Measurable*), pasiekiami (angl. *Achievable*), svarbūs (angl. *Relevant*) ir realizuojami laiku (angl. *Time-bound*). Būda *et al.* (2006) akcentuoja du iš trijų (laikas, kaina, kokybė) prioritetus (2 pav.).



2 pav. Renkantis ne daugiau dviejų – per tam tikrą laiką, už tam tikrus pinigus, pasiekiami tam tikri tikslai

Fig. 2. Choosing no more than two – over certain time, for certain money, certain goals are met

IT projektai yra II ir III tipų. Tokie projektai susiformuoja, kai tikslai būna neaiškūs, bet jų pasiekimo rezultatai apibrėžiami nesunkiai.

Pagal sąvokos *Projektas* apibrėžimą bei jo analizę – projekto metu sukurto rezultato vystymas ir tobulinimas nėra projektas. Taigi bendra projekto veikla yra aiškiai apibrėžiama į dvi dalis:

- projekto kūrimas;
- rezultato vystymas ar administravimas.

Analizuojant šias dvi atskiras dalis saugumo (toliau – saugos) atžvilgiu, problema kyla dėl vienos ir kitos dalies tarpusavio nesuderinamumo. Kuriant IT projektą, yra išpildoma bendrojo saugumo dalis – *de facto* (jeigu projekto koncepcijoje nėra numatyti saugumo standartai sistemai, bet straipsnyje kalbama apie sistemas, kurios standartiškai naudoja *de facto* saugumo taisyklių rinkinį), tačiau vystant ar administruojant rezultatą (dažniausiai jau net ir kitoms šalims, nei projekto kūrimas) iškyla nepatogumai: norint prieiti prie sistemos taško (pvz., nutolusio), reikia įveikti daugybę saugumo barjerų. Saugos atžvilgiu tai yra labai gerai – saugos rezultatas pasiektas, tačiau atsitiktinės sistemos klaidos ar vartotojo pagalbos prašymas ir sauga tuo metu tampa nepatogus barjeras, ilginantis gedimo šalinimo reakcijos laiką, taip pat tampantis toks nelankstus, kad dažnai stengiamasi visai nenaudoti bendrojo saugumo. Projekto kūrimo metu išpildžius saugos reikalavimus sunku nustatyti galimus nepatogumus ir keblumus, kad būtų galima „apeiti“ saugą dėl administracinių tikslų, o taisyti šiuos nepatogumus rezultato vystymo ar administravimo metu yra per vėlu: papildomi kaštai, dažnai pačios sistemos architektūros keitimas ir kt.

Ar yra koks nors patikimas būdas ar metodas, kuriuo remiantis būtų galima kurti sistemas saugumo atžvilgiu taip, kad po projekto įgyvendinimo, rezultato vystymo ar administravimo metu nekiltų sunkumų prieiti prie nutolusių taškų ir greitai bei efektyviai šalinti iškilusias vienadienes problemas?

Bendrasis saugumas *de facto*

Informacijos sauga apibrėžiama kaip „aparatiniai ištekliai, programinis tiekimas, procesai ir procedūros, apjungtos informacinių sistemų organizacijoje saugos nuo išorės ir vidaus grėsmių“. Pagrindinė saugumo infrastruktūra, kuri yra standartas *de facto* kuriant sistemas, pateikia vartotojų autentifikavimo ir saugios komunikacijos metodus. Ji remiasi SSL (angl. *Secure Sockets Layer*), PKI (angl. *Public Key Infrastructure*) ir X.509 sertifikatų architektūra. Ši infrastruktūra teikia paslaugas, protokolus ir bibliotekas, kad pasiektų tokius pagrindinius ir būtinuosius saugumo tikslus:

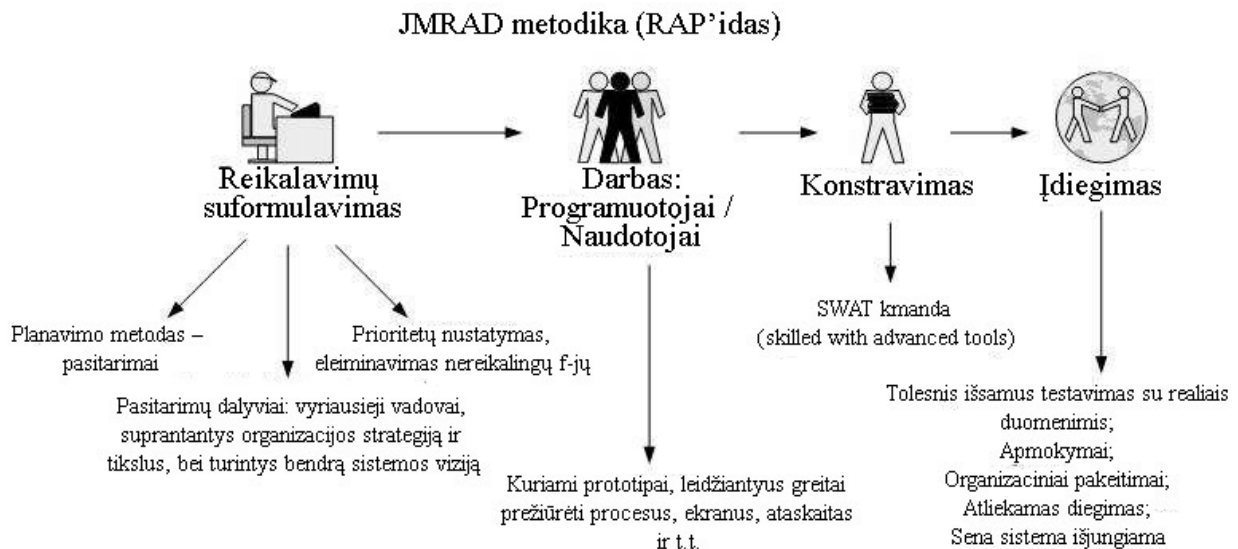
- vienas prisijungimas naudojant paslaugas per vartotojo sertifikatus;
- resursų autentifikavimas per serverio sertifikatus;
- duomenų kodavimas;
- prieigos teisės;
- leidimų ir kontrolės nukreipimas per *proxy* serverius bei patikimų sertifikatų grandinės delegavimas sertifikatų įstaigoms.

De facto taisyklių rinkinys yra ypač naudingas, nes pasaulyje priimto faktinio standarto dar nėra. Jei CobiT (angl. *Control Objectives for Information and related Technology*) netinka, galima naudoti ITIL (angl. *IT Infrastructure Library*), jei NISI (angl. *Network Information Services Infrastructure*) apsaugos vadyba yra netinkama, galima pamėginti ISO 17799. Tačiau reikia naudotis visais, nes vienoje ar kitoje situacijoje tiks vienas iš daug-

lio specifinių standartų. Juolab kad naudojimą reikia planuoti nuolatos: kai projektas kuriamas ir baigiamas, kai prasideda rezultato vystymo ar administravimo dalis.

IT projekto valdymo metodas *JMRAD*

Po teorinės atrankos bei praktinio pritaikomumo pagal šiandienos poreikius (kai norima turėti visus tris 2 pav. iliustruotus prioritetus: laikas, kaina, kokybė) atrinktas metodas yra IT projektuose naudojamas mišrios greito kūrimo metodikos būdas Rapid arba *JMRAD* (angl. *James Martin's Rapid Application Development*). J. Martino sukurta metodika iš esmės yra žinomų ir plačiai taikomų metodų bei priemonių kombinacija (Laučius *et al.* 2007). *JMRAD* metodą galima naudoti, kai verslo tikslai pakankamai gerai žinomi (IT projektuose tikslai dažniausiai kinta pagal inovacijų kiekį rinkoje ir jų pritaikomumą sistemai), duomenys projektui jau egzistuoja, projekto sprendimai gali būti priimti nedidelės grupės žmonių, kurie yra greitai pasiekiami, projekto komanda yra labai maža, projekto techninė architektūra apibrėžta ir aiški, o pagrindiniai technologiniai komponentai yra gerai žinomi. Projekto techniniai reikalavimai: yra normalūs, suderinami su naudojama technologija, intensyvus galutinio vartotojo įtraukimas į sistemos kūrimą *JAD* (angl. *Joint Application Development*). Valdymo procesas, kuris padeda kūrėjų grupėms efektyviai dirbti su vartotojais tam, kad būtų sukurti tinkamiausi IT sprendimai. Tikslas: apibrėžti projektą, sukurti sprendimą ir stebėti projektą, kol jis bus įgyvendintas.



Metodo tikslas: pasiekti apie 80 proc. sistemos funkcionalumo per pirmąsias 90 dienų.

3 pav. *JMRAD* metodikos tikslas pasiekti apie 80 proc. sistemos funkcionalumo per pirmąsias 90 dienų

Fig. 3. The goal of the *JMRAD* methodology is to achieve approx. 80 percent of system functionality in 90 days

JMRAD metodo savybės atitinka visus šiuolaikiškumo (greitai ir efektyviai) reikalavimus ir yra ypatingas tuo, jog tai vienintelė metodika, kuri yra projekto kūrimas bei rezultato vystymas ir administravimas vienu metu (Guelfi *et al.* 2005). JMRAD yra išimtis iš taisyklės: vos pradėjus kurti projektą, jis tuo pat metu yra vystomas bei administruojamas. Vystant yra kuriama pasirinkta saugos schema, kuri tuo pat metu yra ir naudojama: vyksta rezultato administravimas. Susidūrus su kasdienine problema nutolusiam sistemos taške, kuri yra apsaugota *de facto* ar kitomis saugos taisyklėmis, susidūrimo nelankstumas ar nepatogumas yra iškart taisomas projekto vystymo etape ir toliau naudojamas rezultato administravimo dalyje.

Šio metodo susiejimas su specifine saugos problema yra rezultatyvus, tačiau reikalauja greitų ir patikimų sprendimų, pakankamos IT saugos kompetencijos iš projekto vadovų. Laikinoji organizacija (1 pav.) turi neabejoti SWAT (angl. *Skilled With Advanced Tools*) (3 pav., konstravimas) komanda. Vienu metu ir kurti, ir administruoti yra sudėtinga ir pavojinga, todėl JRMAD (Hentzen *et al.* 2002) kritikuojamas dėl metodologijos ir architektūros trūkumo. Idėjos lankstumas mažėja augant programų dydžiui, o metodas gali ir neveikti, jei sistema sąveikauja su kitomis egzistuojančiomis programomis. Metodo našumas ir patikimumas yra kritiniai metodo faktoriai. Sistema negali būti išskaityta į modulius bei turi būti naudojamos tik naujos technologijos (Hoffer *et al.* 2002).

Išvados

1. Atlikta projektų bei informacinių technologijų projektų analizė parodė, kad jų egzistavimą, skirstant į dvi dalis (projekto kūrimas ir rezultato vystymas ar administravimas), saugos politikos taikymas yra mažiau realiai numatomas ir neefektyviai panaudojamas sistemos administravimo metu.
2. Naudojant JRMAD metodą galima efektyviai ir lanksčiai taikyti saugos politiką, atsiradusius keb-

lumus ir nepatogumus greitai šalinti ir taisyti, tačiau paties metodo taikymo taisyklės turi būti griežtos, o komanda profesionali ir patyrusi.

Padėka

Dėkoju prof. habil. dr. Antanui Čeniui už pagalbą rengiant straipsnį.

Literatūra

- Būda, V.; Chmieliauskas, A. 2006. *Projektų valdymas*. Kaunas: Technologija. ISBN 978-9955-25-287-0.
- Guelfi, N.; Savidis, A. 2005. *Rapid integration of software engineering techniques*. Berlin: Springer-Verlag. ISSN 0302-9743. doi:10.1007/b136153
- Hentzen, Wh. 2002. *The Software Developer's Guide*. JAV: Hentzenwerke Publishing. ISBN 1-930919-00-X.
- Hoffer, A. J.; George, F. J.; Valacich, S. 2002. *Modern systems analysis and design*. ISBN 0-8053-2499-2.
- Laučius, J.; Vasilecas, O. 2007. *Informacinių technologijų projektų ir kokybės valdymas*. Vilnius: Technika. ISBN 978-9955-28-146-7.
- Saulis, A.; Vasilecas, O. 2008. *Informacinių sistemų projektavimo metodai*. Vilnius: Technika. ISBN 978-9955-28-345-4. doi:10.3846/1010-S

JRMAD METHOD USES OF INFORMATION TECHNOLOGY SECURITY

E. Švedaitė

Abstract

Analyzing the flexible uses security problems in existing information technology systems. Looking for way to ensure the safety of the reaction time to smooth access to more projects in development. Review of projects undertaken. Codified in the project design and development components. Made of the findings of the methods used to discover, which exclude parts of the draft rule and resort to emergency planning in the early part of the project development phase. Analytical result: JRMAD mixed method, allowing simultaneous two of the project and the time to change the current system.

Keywords: project, safety issues, IT project, JRMAD, security.