VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

Nikolaj GORANIN

GENETINIŲ ALGORITMŲ TAIKYMAS INFORMACIJOS SAUGOS SISTEMOSE

DAKTARO DISERTACIJOS SANTRAUKA

TECHNOLOGIJOS MOKSLAI,
INFORMATIKOS INŽINERIJA (07T)

VGTU
LEIDYKLA
TECHNIKA
Vilnius 2010

Disertacija rengta 2006–2010 metais Vilniaus Gedimino technikos universitete.
Mokslinis vadovas

prof. habil. dr. Antanas ČENYS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, informatikos inžinerija – 07T).

Disertacija ginama Vilniaus Gedimino technikos universiteto Informatikos inžinerijos mokslo krypties taryboje:

Pirmininkas

prof. dr. Dalius NAVAKAUSKAS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, informatikos inžinerija – 07T).

Nariai:

prof. habil. dr. Gintautas DZEMYDA (Matematikos ir informatikos institutas, technologijos mokslai, informatikos inžinerija – 07T),

dr. Algirdas LAUKAITIS (Vilniaus Gedimino technikos universitetas, technologijos mokslai, informatikos inžinerija – 07T),

prof. habil. dr. Rimvydas SIMUTIS (Kauno technologijos universitetas, technologijos mokslai, informatikos inžinerija – 07T),

prof. habil. dr. Rimantas ŠEINAUSKAS (Kauno technologijos universitetas, technologijos mokslai, informatikos inžinerija – 07T).

Oponentai:

prof. dr. Romas BARONAS (Vilniaus universitetas, fiziniai mokslai, informatika – 09P),

dr. Olga KURASOVA (Matematikos ir informatikos institutas, technologijos mokslai, informatikos inžinerija – 07T).

Disertacija bus ginama viešame Informatikos inžinerijos mokslo krypties tarybos posėdyje 2010 m. birželio 11 d. 14 val. Vilniaus Gedimino technikos universiteto senato posėdžių salėje.
Adresas: Saulėtekio al. 11, LT-10223 Vilnius, Lietuva.
Tel.: (8 5) 274 4952, (8 5) 274 4956; faksas (8 5) 270 0112;
el. paštas doktor@vgtu.lt
Disertacijos santrauka išsiuntinėta 2010 m. gegužės 10 d.
Disertaciją galima peržiūrėti Vilniaus Gedimino technikos universiteto (Saulėtekio al. 14, LT-10223 Vilnius, Lietuva), ir Matematikos ir informatikos instituto (Akademijos g. 4., LT-08663 Vilnius, Lietuva) bibliotekose.
VGTU leidyklos „Technika“ 1757-M mokslo literatūros knyga.

© Nikolaj Goranin, 2010

VILNIUS GEDIMINAS TECHNICAL UNIVERSITY

Nikolaj GORANIN

GENETIC ALGORITHM APPLICATION IN INFORMATION SECURITY SYSTEMS

SUMMARY OF DOCTORAL DISSERTATION

TECHNOLOGICAL SCIENCES,
INFORMATICS ENGINEERING (07T)

VGTU
LEIDYKLA
Vilnius TECHNIKA 2010

Doctoral dissertation was prepared at Vilnius Gediminas Technical University in 2006–2010.
Scientific Supervisor
Prof Dr Habil Antanas ČENYS (Vilnius Gediminas Technical University, Technological Sciences, Informatics Engineering – 07T).
The dissertation is being defended at the Council of Scientific Field of Informatics Engineering at Vilnius Gediminas Technical University:
Chairman
Prof Dr Dalius NAVAKAUSKAS (Vilnius Gediminas Technical University, Technological Sciences, Informatics Engineering – 07T).
Members:
Prof Dr Habil Gintautas DZEMYDA (Institute of Mathematics and Informatics, Technological Sciences, Informatics Engineering – 07T),
Dr Algirdas LAUKAITIS (Vilnius Gediminas Technical University, Technological Sciences, Informatics Engineering – 07T),
Prof Dr Habil Rimvydas SIMUTIS (Kaunas University of Technology, Technological Sciences, Informatics Engineering – 07T).
Prof Dr Habil Rimantas ŠEINAUSKAS (Kaunas University of Technology, Technological Sciences, Informatics Engineering – 07T).
Opponents:
Prof Dr Romas BARONAS (Vilnius University, Physical Sciences, Informatics – 09P),
Dr Olga KURASOVA (Institute of Mathematics and Informatics, Technological Sciences, Informatics Engineering – 07T).

The dissertation will be defended at the public meeting of the Council of Scientific Field of Informatics Engineering in the Senate Hall of Vilnius Gediminas Technical University at 2 p. m. on 11 June 2010.
Address: Saulėtekio al. 11, LT-10223 Vilnius, Lithuania.
Tel.: +370 5 274 4952, +370 5 274 4956; fax +370 5 270 0112;
e-mail: doktor@vgtu.lt
The summary of the doctoral dissertation was distributed on 10 May 2010.
A copy of the doctoral dissertation is available for review at the Library of Vilnius Gediminas Technical University (Saulėtekio al. 14, LT-10223 Vilnius, Lithuania) and at the Library of Institute of Mathematics and Informatics (Akademijos str. 4, LT-08663 Vilnius, Lithuania).

© Nikolaj Goranin, 2010

Įvadas

Mokslo problemos aktualumas. Kompanijų ir organizacijų verslo procesai šiuo metu yra labai priklausomi nuo informacinių technologijų infrastruktūros, kuri tampa konkurencingumo ir efektyvumo pagrindu. Kenksmingas programinis kodas (KPK) vertinamas kaip viena pagrindinių grėsmių informacinių resursų konfidencialumui, vientisumui ir prieinamumui. Neigiamas KPK ekonominis poveikis yra ypatingai didelis kaip dėl tiesiogiai padaromos žalos, taip ir dėl išlaidų, kurias kompanijos turi patirti kontrpriemonių diegimui.

Esminiai pasikeitimai KPK kūrėjų motyvacijoje, kai vietoj pripažinimo programišių bendruomenėje pradedama siekti finansinės naudos, daro kiekvieną kompaniją potencialios atakos taikiniu, o apsaugą nuo jo – kritiškai svarbia užduotimi. Tačiau daugeliu atvejų įdiegtos kontrpriemonės būna neefektyvios arba nepakankamos. Pagrindinės to priežastys yra šiuolaikinių antivirusinių paketų priklausomybė nuo parašų duomenų bazės, spragos programinės įrangos atnaujinimo procese, netikslus KPK rizikos vertinimas ir taikytų kontrpriemonių neadekvatumas naujai atsirandančiai grėsmei. Pirmų dviejų problemų sprendimas yra techninėje-organizacinėje plotmėje (euristinių ir anomalijomis paremtų detektavimo metodų taikyme, parašų duomenų bazių ir programinės įrangos procesų optimizavime, griežtos informacinės saugos politikos taikyme) ir intensyvūs tyrimai yra atliekami šioje srityje. KPK rizikos vertinimo bei evoliucijos prognozavimo uždaviniai lieka nepaliesti mokslinių tyrimų ir remiasi tik ekspertų žiniomis bei vertinimais.

Pripažįstama, kad KPK gali būti traktuojamas kaip dirbtinės gyvybės atmaina. Dėl šios priežasties jam gali būti taikomos Darvino evoliucijos taisyklės, nes turimos savybės daugeliu atvejų nulemtos išorinių veiksnių: turimomis technologijomis, keliamais tikslais bei kontrpriemonių poveikiu. Šiame darbe siūlomas genetiniais algoritmais (GA) paremtas KPK rizikos vertinimo ir evoliucijos prognozavimo modelis. Pagrindinis dėmesys skiriamas trims KPK rūšims: interneto kirminams, botnet tinklams ir kodui, plintančiam mobiliuose įrenginiuose. GA pasirinktas kaip modeliavimo įrankis atsižvelgiant į jo gebėjimą atvaizduoti natūralios evoliucijos procesus, efektyvų taikymą optimizavimo ir modeliavimo uždaviniams bei sėkmingus taikymus įvairiose informacinėse saugos sistemose. Modelį sudaro duomenų atvaizdavimo aprašymas, GA parametrai, tikslo funkcija arba vertinimo parametrai.

Tyrimo objektas. Disertacijos tyrimo objektas yra genetinių algoritmų taikymas informacijos saugos sistemose.

Darbo tikslas ir uždaviniai. Pagrindinis darbo tikslas – KPK rizikos vertinimo bei evoliucijos prognozavimo modelio sukūrimas. Darbo tikslui pasiekti reikia išspręsti šiuos uždavinius:

1. Išanalizuoti GA ir jų taikymus įvairiose informacijos saugos sistemose: kriptologinėse, įsiskverbimų detektavimo (IDS), biometrinėse bei kitose.
2. Išanalizuoti egzistuojančius KPK modelius.
3. Išanalizuoti ir aprašyti pasirinktų šiuolaikinių KPK tipų savybes taip, kad jos būtų tinkamos atvaizduoti GA modelyje skirtame KPK rizikos vertinimui ir evoliucijos prognozavimui.
4. Nustatyti tinkamumo vertinimo kriterijus GA paremtam KPK rizikos vertinimo modeliui.
5. Aprašyti ir pagrįsti tikslo (tinkamumo) funkcijas, kurios vertintų kelių KPK tipų 2–3 parametrų evoliucijos tendencijas draugiškoje (kontrpriemonės nėra taikomos) ir priešiškoje aplinkoje (taikomos kontrpriemonės).
6. Įvertinti tikslo funkcijų ir vertinimo kriterijų korektiškumą, pritaikant jas istoriniams duomenims.
7. Apibrėžti GA parametrus, tokius kaip mutacijos tikimybė, kryžminimo tvarka, populiacijos dydis ir kitus.
8. Sukurti modelio prototipą, atlikti eksperimentus su keliais KPK tipais, surinkti ir apdoroti modeliavimo rezultatus.

Mokslinis naujumas. Rengiant disertaciją gauti šie informatikos inžinerijos mokslui nauji GA taikymo teoriniai ir praktiniai rezultatai:

1. Pasiūlytas modelis yra pirmas žinomas KPK modelis, skirtas KPK evoliucijos prognozavimo uždaviniui spręsti.
2. Pasiūlytas automatizuotas KPK rizikos vertinimo metodas paremtas sprendimų medžiais, sugeneruotais GA priemonėmis.
3. Pirmas žinomas GA taikymas KPK evoliucijos prognozavimo uždaviniui spręsti ir automatiniam sprendimų medžių, skirtų naujai atsirandančio KPK rizikos vertinimui, generavimui.

Tyrimų metodika. Norint pasiekti tikslą buvo taikomi šie tyrimų metodai:

1. Lyginamosios analizės ir literatūros analizės metodai buvo taikomi analizuojant GA principus, GA taikymus informacijos saugos sistemose, egzistuojančius KPK modelius ir šiuolaikinio KPK savybes.

2. Apibendrinant analizės rezultatus bei formuluojant pasiūlymus buvo taikomi apibendrinimo ir loginės indukcijos metodai.
3. Eksperimentinio tyrimo metodai buvo taikomi vykdant modelio bandymus.

Praktinė vertė. KPK rizikos vertinimas ir evoliucijos tendencijų prognozavimas yra svarbus moksliniam ekspertų vertinimų pagrindimui, KPK kūrimo tendencijų supratimui, KPK evoliucijos prognozavimui pagal atskirus parametrus arba parametrų kompleksus, kontrpriemonių technologijų kūrimui ir epideminių pasekmių, taikant greitojo reagavimo priemones, mažinimui.

Pasiūlytas modelis buvo pritaikytas Interneto kirminų (iki įsisotinimo, draugiška ir priešiška aplinka), mobilaus KPK (iki įsisotinimo, draugiška aplinka), botnet tinklų (visos plitimo fazės) plitimo strategijų evoliucijos prognozavimui; botnet tinklų (po įsisotinimo, priešiška aplinka) išgyvenamumo savybių evoliucijos modeliavimui ir Interneto kirminų populiacijos stabilumo grėsmės vertinimui. Gauti modeliavimo rezultatai leido įvertinti skirtingas KPK strategijas bei daryti prielaidas dėl nurodytų KPK tipų evoliucijos tendencijų.

Pasiūlyto modelio pritaikomumas priklauso nuo naudojamų statistinių duomenų patikimumo. Modelis gali būti išplečiamas kitiems KPK tipams arba jų parametrams, papildant funkcijų aprašymus chromosomoje bei atnaujinant tikslo funkciją.

Ginamieji teiginiai. Remiantis tyrimų rezultatais gali būti suformuluoti šie ginamieji teiginiai:

1. GA taikymas leidžia modeliuoti kenksmingo programinio kodo evoliucijos tendencijas.
2. Sprendimų medžių, sugeneruotų GA priemonėmis, taikymas, leidžia automatizuoti kenksmingo programinio kodo keliamos rizikos vertinimo procesą.
3. Pasiūlytas GA paremtas kenksmingo programinio kodo rizikos ir evoliucijos prognozavimo modelis gali būti pritaikytas kitiems kenksmingo programinio kodo tipams ir/ar jų parametrams.

Darbo apimtis. Darbą sudaro įvadas, keturi pagrindiniai skyriai ir bendrosios išvados. Darbo apimtis yra 115 puslapių, tekste panaudotos 40 numeruotos formulės, 30 paveikslų ir 7 lentelės. Rašant disertaciją buvo panaudoti 169 literatūros šaltiniai. Darbas buvo pristatytas 6 konferencijose. Disertacijos tema publikuoti 7 straipsniai.

1. Genetiniai algoritmai ir jų taikymas informacijos saugos sistemose

Pirmame skyriuje pateikiama bendrų GA principų ir GA taikymo informacijos saugos sistemose, tokiose kaip biometrinės autentifikacijos sistemos, kriptologiniai sprendimai, įsiskverbimų detektavimo sistemos, o taip pat ir kitose sistemose, analizė. Ypatingas dėmesys yra skiriamas GA atvaizdavimo metodams ir algoritmų parametrų priklausomybei nuo sprendžiamo uždavinio: chromosomų formavimui, tikslo funkcijoms arba vertinimo kriterijams, kryžminimo ir mutacijos parametrams ir kt. Neuro-genetinis metodas taip pat analizuojamas, remiantis keliais pavyzdžiais. GA taikymo tikslingumas kiekvienai iš aprašomų sričių yra pateikiamas ir perspektyviausios tyrimo kryptys GA taikymo informacijos saugos srityje yra apibrėžiamos.

Literatūros analizė parodė, kad pagrindiniai GA taikymo tyrimai informacinės saugos srityje yra orientuoti į taikymus kriptologijoje, IDS ir biometrinėse autentifikacijos sistemose. Yra publikuoti tik keli straipsniai, kuriuose nagrinėjami GA taikymai informacinės saugos procesų modeliavimo uždaviniui spręsti. Kriptologiniai GA taikymai gali būti vertinami kaip įdomūs, tačiau neturintys didelės praktinės reikšmės, kadangi siūlomi tik su standartais nesuderinti patobulinimai egzistuojantiems šiuolaikiniams šiframs, o GA paremtos atakos neaktualios, kadangi taikomos prieš klasikinius (perstatymo, sumaišymo), jau pripažintus nesaugiais („lengvoji“ ir Merkle-Hellman kuprinės) arba nepopuliarius (Chor-Rivest) šifrus. GA aktyviai taikomi IDS sistemose, bet siūlomi sprendimai neperžengė mokslinių tyrimų ir prototipų bandymų ribos, dažnai būna siaurai specializuoti. Tyrimai vertinami kaip perspektyvūs, kadangi sukurti prototipai demonstruoja aukštą efektyvumo lygį ir gali būti optimizuoti, parenkant GA parametrus. Perspektyviais gali būti laikomi ir GA taikymai biometrinėse sistemose, nors dauguma sukurtų sistemų taip pat yra prototipo kūrimo fazėje. GA taikymas leidžia kokybiškai pagerinti biometrinių sistemų parametrų, tokių kaip greitis, klaidų skaičius ir lankstumas, rodiklius. Pagrindiniai tyrimai daromi piršto atspaudų ir veido bruožų apdorojimo srityje, egzistuoja darbai, kur analizuojami GA taikymai kitų biometrinių parametrų apdorojimui.

Analizės metu nustatyta, kad GA gali būti taikomi užsibrėžtam tikslui pasiekti, atsižvelgiant į metodo gebėjimą imituoti evoliucijos procesus, sėkmingus taikymus sprendžiant optimizavimo uždavinius ir uždavinius su didele sprendimų aibe. Analizė taip pat parodė, kad šiuo metu nėra egzistuojančio sprendimo, kurį būtų galima taikyti KPK rizikos vertinimui ir evoliucijos prognozavimui. Remiantis atliktos analizės rezultatais formuluojami disertacijos uždaviniai.

2. Kenksmingo programinio kodo techninė analizė ir kenksmingo programinio kodo modeliai

Skyriuje aprašomos trijų pasirinktų šiuolaikinių KPK tipų savybės. Pateikiama interneto kirminų, vertinamų kaip viena agresyviausių KPK rūšių, sąlyginai naujo mobilaus KPK ir greitai evoliucionuojančių botnet tinklų, kurie traktuojami kaip didžiausia grėsmė informacinei saugai, techninė analizė, kuri apima KPK tipo ir kelių tipinių atstovų apžvalgą. KPK mechanizmų veikimo supratimas yra būtinas jas pateikiant GA tinkamu formatu. Nustatyta, kad beveik visas šiuolaikinis KPK yra kuriamas moduliniu principu. Palaikomos savybės priklauso nuo atakuojamos sistemos ir tikslų, priskirtų KPK kūrėjo, besiremiančio intuiciją ir aplinkos, kurioje turės veikti KPK, sąlygų vertinimu. Įvedamas KPK strategijos, kaip metodų ir savybių rinkinio, apibrėžimas.

Analizuojami egzistuojantys KPK modeliai, siekiant palyginti jų savybes ir efektyvumą su siūlomu GA paremtu KPK rizikos vertinimo ir evoliucijos prognozavimo modeliu. Analizės metu nustatyta, kad egzistuojantys KPK modeliai koncentruojasi ties epideminių pasekmių modeliavimu, t.y. užkrėstų kompiuterių populiacijos dydžio nustatymu, KPK elgesio modeliavimu arba KPK plitimo ekonominiais aspektais, ir remiasi tik egzistuojančiomis KPK strategijomis. Vienintelis egzistuojantis GA paremtas modelis yra skirtas evoliucijos galimybės demonstracijai ir negali būti taikomas evoliucijos tendencijoms nustatyti, kadangi nėra siūlomi evoliucijos vertinimo mechanizmai, bet kai kurie pasiūlyti sprendimai, tokie kaip aukšto lygio genotipo atvaizdavimas, labai panašūs į šiame darbe pateiktus siūlymus ir demonstruoja pasirinktos tyrimų krypties aktualumą ir perspektyvumą.

3. Automatinis kenksmingo programinio kodo rizikos vertinimo modelis

Trečiame skyriuje pateikiamas KPK rizikos vertinimo modelis ir jo pritaikymas interneto kirminų populiacijos stabilumo grėsmei įvertinti po įsisotinimo fazės. Siūlomas modelis yra paremtas sprendimų medžiais, kuriamais klasifikuotų istorinių duomenų pagrindu. Sprendimų medžių generavimui yra naudojama GA paremta GAtree programinė įranga. Istoriniai duomenys traktuojami kaip sugeneruotų sprendimų medžių vertinimo kriterijus. GAtree veikimas remiasi klasikiniu GA algoritmu, tačiau chromosomos atvaizdavimas pakeistas iš dvejetainio į medžio pavidalą.

Eksperimento metu GAtree programai buvo pateiktas 100 duomenų įrašų mokomasis struktūrizuotas tekstinis duomenų rinkinys. Duomenų įrašo struktūrą sudarė sekantys interneto kirmino strategiją aprašantys laukai: *OS_PLATF* (palaikoma operacinė sistemą); *EXPL_1–EXPL_N* (naudojami

užkratai); *IP_GEN* (atakuojamo kompiuterio IP adreso generavimo būdas); *TRANSF* (kirmino kūno pristatymo būdas); *MEM* (naudojamos atminties tipas); *HIER* (palaikomos hierarchijos tipas); *COM* (užkrėstų kompiuterių tarpusavio bendravimo mechanizmas); *EXEC* (kirmino valdymo funkcijos); *ADD* (papildomos kirmino funkcijos); *EVOL* (kirmino evoliucionavimo galimybės) ir populiacijos mažėjimo greičio kategorija (Low; Medium-low; Medium; Medium-high; High), kuri nurodo procentaliai populiacijos sumažėjimą nuo įsisotinimo fazės pabaigos per vieno mėnesio laiko tarpą. Geriausio sugeneruoto medžio (fragmentas pateiktas 1 pav.) įvertinimas buvo lygus 0,571, vidutinis medžių populiacijos įvertinimas – 0,517.

```
...

| | |-'Low'
| | +-if HIER='Centralized hierarchy' then
| |   |-if COM='child-parent' then
| |   | |-'Medium'
| |   +-'Medium-low'
| +-'Low'
+-if TRANSF='UDP' then
  |-'Low'
  +-if MEM='-' then
    |-'Low'
    +-'Medium-low'
...
```

1 pav. Rizikos vertinimo sprendimo medžio fragmentas

Sugeneruoto geriausio sprendimo medžio efektyvumas buvo vertinamas pateikiant klasifikavimui 5 interneto kirminų strategijų pavyzdžius, neįtrauktus į klasifikuotų duomenų rinkinį. Testinės strategijos buvo klasifikuotos tiksliai, taip patvirtinant modelio korektiškumą. Pasiūlytas automatinis KPK rizikos vertinimo modelis gali būti traktuojamas kaip pirmas automatinis sprendimas naujai atsirandančio KPK rizikai nustatyti, priešingai šiuo metu taikomiems ekspertų vertinimams. Norint pritaikyti šį modelį kito tipo rizikai įvertinti, užtenka įrašytoms į duomenų rinkinį strategijoms priskirti naujas klasifikavimo kategorijas ir automatiškai pergeneruoti sprendimų medžius, tuo tarpu strategijų atvaizdavimas liktų nepakitęs.

4. Kenksmingo programinio kodo evoliucijos prognozavimo modelis

Skyriuje aprašomas GA paremtas KPK evoliucijos prognozavimo modelis. Modelyje GA imituoja evoliucijos procesus KPK vystimosi tendencijoms nustatyti. KPK efektyvumo optimizavimo parametrus yra bandoma vertinti KPK kūrėjų akimis, norint gauti objektyvius modeliavimo rezultatus. Aprašomą

modelį sudaro trys pagrindinės dalys: chromosomos, atvaizduojančios KPK savybes, struktūros aprašymas, tikslo (tinkamumo) funkcija ir GA parametrai, tokie kaip populiacijos dydis, tėvų atrankos metodai ir kt. Kiekviena KPK strategija atvaizduojama kaip chromosoma, sudaryta iš genų, savo ruožtų aprašančių vieną ar kitą strategijoje naudojamą metodą. Pradinė sprendimų populiacija generuojama atsitiktinai, vertinamas sugeneruotų strategijų tinkamumas, ir jei nėra pasiekiama nutraukimo sąlyga, paleidžiami evoliuciniai operatoriai (kryžminimas, mutacija). Procesas kartojamas, kol nėra pasiekiama nutraukimo sąlyga. Kaip ir daugelio kitų prognozavimo modelių atveju, kurie negali būti įvertinti eksperimentiškai (pvz., klimato kaitos), modelio korektiškumas vertinamas pritaikant jį istoriniams duomenims, t. y. skaičiuojant tikslo funkcijos reikšmę tiems KPK, kurių tinkamumo reikšmė yra žinoma. Nustatyti neatitikimai (mažesni nei 0,01) buvo įvertinti kaip neesminiai.

Interneto kirminų evoliucijos modeliavimas

Eksperimento tikslas buvo maksimizuoti kirmino plitimo greitį nustatytu laikotarpiu (iki įsisotinimo fazės). Interneto kirmino savybes aprašanti chromosoma yra sudaryta iš 30 genų, dalis kurių yra visada aktyvūs (yra gyvybiškai svarbūs arba aktyvuoja/deaktyvuoja kitus genus) ir aktyvuojamus. Toks atvaizdavimas leidžia atvaizduoti visas kirminų savybes ir užtikrinti fiksuotą chromosomos ilgį. Pavyzdinė strategija pateikta 2 paveiksle.

```
S_i=(IP_GEN="Random,   excluding   127.0.0.0/8,   loopback,
224.0.0.0/8,     multicast";     OS_PLATF="Apple     OS";
TRANSF="Connection  oriented";  EXPL_1="  CVE-2007-3876";
EN_EXPL_2="False";  EN_EXPL_3="False";  EN_EXPL_4="False";
EN_EXPL_5="True";   EN_EXPL_6="False";   EN_EXPL_7="False";
EN_EXPL_8="False";   EXPL_2="-";   EXPL_3="-";   EXPL_4="-";
EXPL_5="    CVE-2004-0485";    EXPL_6="-";    EXPL_7="-";
EXPL_8="-";   EN_MEM="False";   MEM="-";   EN_HIER="True";
HIER="Autonomous";         EN_COM="False";         COM="-";
EN_EXEC="True";         EXEC="Update        functionality";
EN_ADD="True"; ADD="Write to MBR to remain after reboot";
EN_EVOL="False"; EVOL="-")
```

2 pav. Pavyzdinė atsitiktinai sugeneruota interneto kirmino strategija

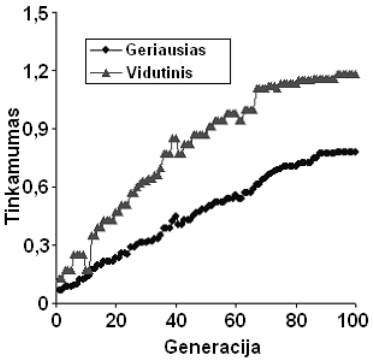
Populiacijos dydis N – 50, išlieka stabilus po kiekvienos generacijos. Taikoma kombinuota nutraukimo sąlyga: algoritmo veikimas nutraukiamas jei pasiekiama 100 generacijų arba evoliucijos stagnacija 10 generacijose iš eilės. Kryžminimo taško pasirinkimas atsitiktinis, mutacijos tikimybė – 0,005, naudojama proporcinė tėvų atranka. Tinkamumo vertinimas remiasi Atsitiktinio pastovaus plitimo (*angl.* Random Constant Spread) modelio prielaida, kad kuo

didesnis yra kirmino parametras *K*, nurodantis vidutinį užkrėčiamų kompiuterių skaičių, tuo greičiaus didės kirmino populiacija. Darbe siūlomi *K* parametro skaičiavimai remiasi laiko sąnaudų kirmino funkcijų įvykdymui ir aukos užkrėtimo tikimybės vertinimu:

$$K(S) = k \cdot p_1^S \cdot p_2^S \cdot p_3^S \sum_{i=4}^{30} p_i^S; \qquad k = \frac{1}{\sum_{j=1}^{30} t_j^S}, \tag{1}$$

čia: *S* – vertinama strategija; p_1^S – tikimybė, kad sugeneruotas IP adresas egzistuoja ir yra aktyvus, p_2^S – tikimybė, kad aukos kompiuteryje veikia palaikoma operacinė sistema, p_3^S – tikimybė, kad kirminas bus sėkmingai pristatytas iki aukos kompiuterio, p_i^S – tikimybė, kad genų (Nr. 4–30) veikimo rezultatu bus aukos infekavimas, *k* – ciklų skaičius, kuriuos kirminas atlieka per vieną sekundę, t_j^S – laiko sąnaudos, reikalingos geno funcionalumui įvykdyti. Padaroma prielaida, kad užkrėtimo tikimybės yra sąlyginai mažos (<0,05), o kirmino kūnas gali būti pristatytas iki aukos kaip TCP, taip ir UDP protokolu.

Modeliavimo metu buvo atlikta 10 bandymų. Didžiausia gauta *K* reikšmė buvo lygi 1,18, kuri atitiko strategiją, pagrįstą Windows OS platformos naudojimu, atsitiktinių IP adresu generavimu (išmetant 127.0.0.0/8, loopback, 224.0.0.0/8, multicast), UDP pristatymo mechanizmu, 4 užkratais (*angl.* exploit) su aukšta užkrėtimo tikimybe ir visais kitais deaktyvuotais genais. Geriausio individo ir vidutinės strategijos tinkamumo kitimas parodytas 3 paveiksle.



3 pav. Populiacijos ir geriausio individo tinkamumo keitimasis (interneto kirminai)

Esant priešiškai aplinkai (taikomos kontrpriemonės), $K(S)$ tikimybės tampa priklausomos nuo laiko, išskyrus p_2^S (nykstamai mažas vartotojų skaičius keis operacinę sistemą atsiradus naujam kirminui), ir laikui bėgant plitimo greitis mažėja, o dėl kontrpriemonių taikymo kompleksiškumo tektų naudoti statistinius duomenis aproksimuojančią funkciją. Tuomet strategijos efektyvumui įvertinti galima naudoti išvestinę pagal laiką:

$$F_{SC}\left(K_S\left(t\right)\right)=\frac{dK_s(t)}{dt}, \tag{2}$$

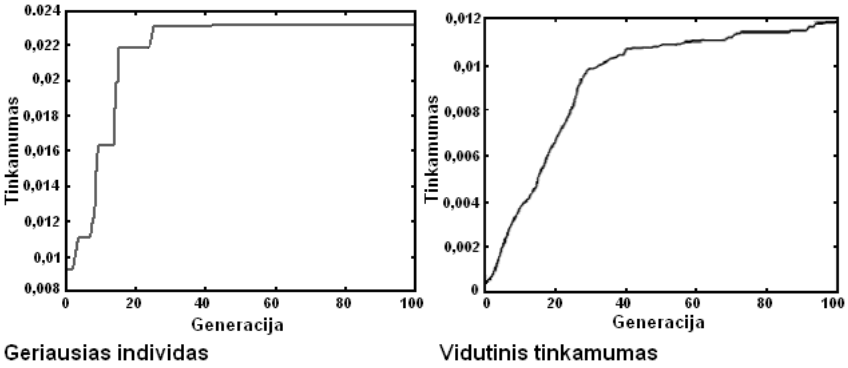
kuri rodo strategijos efektyvumo kritimo greitį. Dėl patikimų statistinių duomenų trūkumo darbe yra pateikiamas tik tikslo funkcijos pagrindimas be eksperimento rezultatų.

Mobilaus kenksmingo programinio kodo evoliucijos modeliavimas

GA parametrai mobilaus KPK evolicijai modeliuoti atkartoja naudojamus interneto kirminų evoliucijos prognozavimo modelyje, tačiau yra pašalinti apribojimai dėl tikimybių dydžių. Strategijos atvaizdavime yra įtraukti papildomi genai arba jų reikšmės, aprašantys specifines mobilaus KPK savybes: plitimo metodus (MMS, SMS, kt.), mobilių įrenginių platformas ir operacines sistemas, veikimo uždelsimą ir kt. Maksimizuojant plitimo greitį draugiškoje aplinkoje iki įsisotinimo fazės siūloma taikyti šią tikslo funkciją:

$$\begin{aligned} K(S) = k \cdot & \left(\begin{array}{l} 1-\left(1-p_6^S\left(NR\_TIME\right)\right)\cdot\left(1-p_7^S\left(BT\_TIME\right)\right) \\ \cdot\left(1-p_8^S\right)\cdot\left(1-p_9^S\left(WIFI\_TIME\right)\right) \end{array} \right) \\ & \cdot p_{10}^S \cdot p_{11}^S \cdot \left(1-\prod_{i=15}^{17}\left(1-p_i^S\right)\right) \end{aligned} \tag{3}$$

čia: S – vertinama strategija; p_6^S–p_9^S – tikimybės, kad užkratai bus sėkmingai pristatyti (p_6^S, p_7^S ir p_9^S priklauso nuo laiko); p_{10}^S – tikimybė, kad atakuojamame įrenginyje bus įdiegta palaikoma OS; p_{11}^S – tikimybė, kad įrenginys yra palaikomas; p_{15}^S -p_{17}^S – tikimybės, kad atakuojama sistema bus infekuota (užkratu); k – ciklų skaičius, kuriuos mobilus KPK atlieka per vieną sekundę (skaičiavimas analogiškas interneto kirminų atvejui). Geriausio individo ir populiacijos vidutinio tinkamumo kitimas parodytas 4 paveiksle.



4 pav. Populiacijos ir geriausio individo tinkamumo keitimasis (Mobilus KPK)

Geriausios strategijos įvertinimas buvo lygus $K(S_d) = 0{,}023$. Modeliavimas parodė, kad ateityje mobilus KPK be šiuo metu įprastu funkcijų ir savybių palaikys Win Mobile šeimos OS bei plitimo Wi-Fi tinklais galimybę.

Botnet tinklų evoliucijos modeliavimas

Botnet tinklų modelio parametrus siūloma parinkti, naudojant patikimą statistiką, leidžiančią vertinti atskirų botnet savybių laiko sąnaudas ir efektyvumą. Deja, kol kas tokia statistika nėra sukaupta. Chromosomoje, sudarytoje iš 7 genų (*TARGET_SEARCH; TRANSF; EXPL_PLATF; EXPL_NUM; HIERARCHY; FUNCTIONALITY; SELF_PROTECT*), atsižvelgiant į KPK tipo sudėtingumą ir lankstumą, realizuota nuorodų į metodus ir savybes sistema, leidžianti naudoti kelis aukos paieškos metodus, kelias OS platformas, iki 81 užkrato.

Maksimizuojant populiacijos plitimo greitį siūloma naudoti tikslo funkciją, analogiška mobiliam KPK, atvaizduojančią pakitimus chromosomos struktūroje:

$$K(S) = k \cdot k_1 \cdot k_2 \cdot k_3 \cdot \left(1 - \prod_{i=1}^{9}\left(1 - p_i^{1,S}\right)\right) \cdot \left(1 - \prod_{i=1}^{9}\left(1 - p_i^{2,S}\right)\right) \cdot \left(1 - \prod_{i=1}^{9}\left(1 - p_i^{3,S}\right)\right) \cdot \left(1 - \prod_{i=1}^{9}\prod_{j=1}^{E[i]}\left(1 - p_{ij}^{4,S}\right)\right), \quad (4)$$

čia: S – vertinama strategija; p_i^1 – aktyvios aukos i^{uoju} metodu radimo tikimybė; p_i^2 – užkrato pristatymo i^{uoju} metodu tikimybė; p_i^3 – palaikomos platformos radimo i^{uoju} metodu tikimybė; p_{ij}^4 – tikimybė, kad j^{asis} užkratas (iš $E[i]$ užkratų, palaikomų i^{uoju} metodu, užkrės aukos kompiuterį; k – ciklų skaičius per minutę; k_1–k_3 – tiesioginiai neįtakojančių užkrėtimo tikimybės genų poveikio plitimui koeficientai. Siūloma formulę taikyti visais plitimo etapais, perkeliant 25 % geriausių strategijų į kitą etapą.

Norint įvertinti botnet strategijas, užtikrinančias botnet tinklo populiacijos išgyvenamumą laiko intervalu T_S, siūloma taikyti šią tikslo funkciją:

$$F(S) = k \cdot \prod_{i=1}^{9} \left(1 - p_i^S \left(self\_protect\right)\right), \tag{5}$$

čia: S – vertinama strategija; p_i^S – tikimybė, kad i^{asis} metodas (*SELF_PROTECT*) apsaugos botnet mazgą nuo detektavimo ir pašalinimo, k – botnet mazgo aktyvumo lygis, skaičiuojamas pagal formulę:

$$k = \frac{t(S)}{T_S}; \qquad t(S) = \sum_{j=1}^{7} \sum_{i=1}^{9} t_i^S \cdot \frac{CPU\_LOAD_i}{100\,\%}, \tag{6}$$

čia: $t(S)$ yra suminės strategijos S metodų laiko sąnaudos vertinamu periodu T_S, t_i^S – konkretaus metodo laiko sąnaudos, o CPU_LOAD_i – vidutinis kompiuterio procesoriaus apkrovimas. Dėl patikimų statistinių duomenų trūkumo darbe yra tik pateikiamas botnet evoliucijos modelio aprašymas be eksperimentinių bandymų rezultatų.

Bendrosios išvados

1. Remiantis atliktais vertinimo testais, buvo patvirtintas principinis siūlomo kenksmingo programinio kodo rizikos vertinimo modelio, naudojančio genetinio algoritmo priemonėmis sugeneruotus sprendimų medžius naujai atsirandančio kenksmingo programinio kodo keliamai rizikai nustatyti, korektiškumas. Modelis gali būti rekomenduotas įspėjimo apie kenksmingo programinio kodo grėsmę sistemų automatizavimui.
2. Perspektyvių interneto kirminų strategijų, siekiančių maksimizuoti infekuotų kompiuterių skaičių per ribotą laiko intervalą, evoliucijos modeliavimas parodė tokias tendencijas: Interneto kirminai evoliucionuos link paprastų sprendimų, atakuojančių vieną

populiariausią operacinių sistemų platformą, naudojančių UDP pristatymo mechanizmus (“iššoviau ir pamiršau” principas) ir kombinaciją iš 4–5 užkratų, turinčių aukštą infekavimo tikimybę. Apskaičiuotas geriausios strategijos, gautos eksperimento metu, tinkamumas, buvo lygus 1,180. Lyginant su interneto kirmino Code Red v.2 tinkamumu (0,015) tinkamumas padidėjo 79 kartus.

3. Perspektyvių mobilaus kenksmingo programinio kodo strategijų, siekiančių maksimizuoti infekuotų kompiuterių skaičių per ribotą laiko intervalą, evoliucijos modeliavimas parodė, kad mobilaus KPK evoliucija vystysis kelių operacinių sistemų platformų palaikymo linkme, bus taikomas plitimas WI-FI tinklais (šiuo metu dominuoja MMS ir Bluetooth plitimo metodai) bei bus atsikratoma papildomų funkcijų. Prognozuojamos strategijos tinkamumas lyginant su pavyzdine egzistuojančia padidės 1,7 kartų.
4. Vertinant sumodeliuotas evoliucijos tendencijas nustatyta, kad ateities kenksmingo programinio kodo epidemijos turės didesnių neigiamų pasekmių, nei sukeltos šiuolaikinio kenksmingo programinio kodo, todėl nauji bei patobulinti apsaugos metodai, tokie kaip kenksmingo programinio kodo detektavimas ir blokavimas tinklo sraute, anomalijomis paremti detektavimo mechanizmai, tinklo infrastruktūros balansavimas turi būti taikomi norint jas minimizuoti.

Autoriaus publikacijų disertacijos tema sąrašas
Recenzuojamuose mokslo žurnaluose

Goranin, N.; Cenys, A. 2008a. Genetic Algorithm Based Internet Worm Propagation Strategy Modeling, *Information Technology and Control* 37(2): 133–140. ISSN 1392-124X (ISI Web of Science)

Goranin, N.; Cenys, A. 2008b. Malware Propagation Modeling by the Means of Genetic Algorithms*, Elektronika ir elektrotechnika* 6(86): 23–26. ISSN 1392-1215 (ISI Web of Science)

Goranin, N.; Cenys, A. 2009. Genetic Algorithm Based Internet Worm Propagation Strategy Modeling Under Pressure of Countermeasures, *Journal of Engineering Science and Technology Review* 2(1): 43–47. ISSN 1791-2377

Straipsniai kituose leidiniuose

Goranin, N.; Cenys, A.; Juknius, J. 2010. Extension of the Genetic Algorithm Based Malware Strategy Evolution Forecasting Model for Botnet Strategy Evolution Modeling, in *Proc. of NATO RTO Information Systems Technology Panel Symposium, Information Assurance and Cyber Defense* (IST-091 / RSY-021), Antalya. Turkey. RTA-NATO, P8-1–P8-20.

Juzonis, V.; Goranin, N.; Cenys, A. 2010. Genetic Algorithm Modelling Approach for Mobile Malware Evolution Forecasting, in *Proc. of the 16th International Conference on Information and Software Technologies*, Kaunas, 259–264. ISSN 2029-0063.

Goranin, N.; Cenys, A. 2008c. Analysis of Malware Propagation Modeling Methods, in *Proc. of the Eleventh Lithuanian Conference of Young Scientists Science – Future of Lithuania*. Vilnius: Technika, 428–434. ISBN 978-995-52830-2-7.

Goranin, N.; Cenys, A. 2007. Genetic Algorithm Application in Cryptography and Cryptology (Genetinių algoritmų taikymas kriptografijoje ir kriptoanalizėje), in *Proc. of the Tenth Lithuanian Conference of Young Scientists Science – Future of Lithuania*. Vilnius: Technika, 527–533 (in Lithuanian). ISBN 978-995-52814-4-3.

Trumpos žinios apie autorių

Nikolaj Goranin gimė 1981 m. lapkričio 26 d. Vilniuje. 2004 m. įgijo informatikos inžinerijos bakalauro laipsnį Vilniaus Gedimino technikos universiteto (VGTU) Fundamentinių mokslų fakultete. 2004 m. stažavosi ES Jungtinių tyrimų centro IPSC instituto CyberSecurity laboratorijoje. 2006 m. įgijo informatikos inžinerijos mokslo magistro laipsnį VGTU. Turį darbo patirties kaip sistemų administratorius, informatikos mokytojas, ES FP6 ir struktūrinių fondų projektų koordinatorius, verslo procesų saugos vadovas. 2006–2010 m. – VGTU doktorantas. Šiuo metu dirba asistentu ir jaunesniuoju mokslo darbuotoju VGTU Informacinių sistemų katedroje ir Informacinių technologijų saugos mokslo laboratorijoje.

GENETIC ALGORITHM APPLICATION IN INFORMATION SECURITY SYSTEMS

Topicality of the problem. Business processes of companies and organizations nowadays are highly dependant on the information technology infrastructure. To remain competitive and effective so should be their information systems. Malware is considered to be among the biggest threats to information resources availability, confidentiality and integrity. The negative malware economic effect is extremely high, due to both direct harm done by malware and expenses the companies have to spend on countermeasures.

Significant changes in malware creators' motivation from recognition in hacker community to financial gain make every company a potential victim, and the protection against malware a crucial task. Still in many cases countermeasures implemented remain inefficient or insufficient. The main reasons for this are dependence of current antivirus software on signature databases, gaps in the software update process, incorrect evaluation of the threat

posed by a specific malware and inadequacy of countermeasures implemented to a threat caused by a new malware. While the solution of the first two problems lays in technical-organizational area (usage of heuristic or anomaly based malware detection methods, optimisation of signature database and software patch management process, implementation of strict information security standards) and an intensive research is done to improve technical characteristics of antivirus software, the malware risk level evaluation and evolution forecasting tasks remain uncovered by scientific models and rely on empirical expert knowledge and evaluation, although many malware researchers recognize the fact that creation of such model would be important both from practical and scientific point of view. Existing malware models mainly concentrate on other tasks.

It is widely accepted that malware can be considered as a form of artificial life. Due to that reason it should follow the general Darwinian evolution rules, since methods implemented by malware creators in malware are forced by external factors: available technology, tasks assigned and countermeasures.

In this research we propose using the genetic algorithm (GA) modelling approach for malware risk level evaluation and evolution forecasting. The main attention is dedicated to three malware types: Internet worms, botnets and mobile malware. The GA is selected as a modelling tool taking into consideration its ability to simulate natural evolution processes, efficiency while solving optimisation, modelling problems with large solution space and successful application for other information security tasks. The model includes the GA description, operating conditions, chromosome that describes malware characteristics, the fitness function for evolution forecasting or evaluation criteria for risk level evaluation and the modelling platform.

The object of research. The object of present study is application of genetic algorithms in information security systems.

Main objective and tasks of the work. The main objective is creation of malware risk level evaluation and malware evolution forecasting model. In order to achieve the objective, the following problems had to be solved:

1. To review GA and their application in different information security areas such as cryptology, intrusion detection systems, biometry and others.
2. To analyse existing malware models.
3. To analyse and describe features of selected modern malware types in the way suitable for representation in GA model, dedicated to risk level evaluation and evolution forecasting.

4. To derive fitness evaluation criteria for GA based malware risk level evaluation model.
5. To derive a fitness functions 2–3 parameters evolution tendencies forecasting of several malware types in a friendly (no countermeasures applied) and, where applicable, hostile (countermeasures applied) environment.
6. To evaluate correctness of the fitness functions and fitness evaluation criteria by applying them to historical data.
7. To define GA operation conditions such as mutation, crossover operators, population size, etc.
8. To develop the model prototype, perform experiments on several malware types, collect and evaluate modelling results.

Importance of scientific novelty. The aspects of scientific novelty on theoretical and experimental investigation of GA application for malware risk level evaluation and evolution forecasting are as follows:

1. The model proposed is the first known malware model dedicated to malware evolution forecasting task.
2. The automated method of malware risk evaluation, based on decision tree generation by GA, was proposed.
3. The first known application of GA for malware evolution forecasting task and automatic classifying tree generation, dedicated to new malware risk level evaluation.

Research methodology. To achieve the objective, the following research methods were used:

1. Comparative research and literature research methods were used while analysing the GA principles, their applications in information security systems, existing malware models and modern malware techniques.
2. The analysis results were summarized and the approach was expounded using the research generalization and logical induction methods.
3. The experiment research method was applied while performing the model tests.

Practical significance of achieved results. Malware risk level evaluation and forecasting evolution tendencies is important for scientific substantiation of expert prediction evaluation, understanding of malware development tendencies, malware evolution forecasting by separate parameters or their

complexes, development of countermeasure techniques and prevention of malware epidemic outbreaks by implementing quick response mechanisms.

The proposed model was applied for Internet worms propagation strategy evolution forecasting (prior to satiation, both friendly and hostile environments), mobile malware (prior to satiation, friendly environment) and botnets (all propagation phases, friendly environment), for botnet survivability evolution forecasting (after satiation, hostile environment) and for evaluation of Internet worm population stability threat evaluation and certain results were achieved, that allowed us to make evaluation about evolution tendencies of these malware types.

The applicability of the proposed model is highly dependent on the collection of the reliable statistical data. The proposed model is easily extensible for other malware types and parameters so only minor modifications should be made to apply the model for other malware types and parameters evolution forecasting.

The defended statements. The following statements based on the results of present investigation may serve as the official hypotheses to be defended:

1. Application of GA allows forecasting malware evolution tendencies.
2. GA approach for decision tree, dedicated to malware risk level evaluation, generation, allows automatic malware risk level evaluation.
3. The proposed GA based malware risk level evaluation and evolution forecasting model is expandable for different malware types and malware parameters.

The scope of the scientific work. The dissertation is composed of Introduction, four main chapters and general conclusions. The total dissertation scope is 115 pages, 30 pictures and 7 tables.

In Introduction topicality of the problem is analysed, work main objective and tasks are formulated, scientific novelty is proved, research methods used are listed and defended statements are presented.

Chapter 1 provides the analysis of GA general principles and their application in information security systems such as biometric authentication systems, cryptology, intrusion detection systems and others. Special attention is dedicated to GA representation methods and operating conditions dependability on the task solved: chromosome formatting methods, fitness functions or evaluation criteria, crossover and mutation parameters, etc. Neuro-genetic approach is also analysed on set of examples. Expediency of GA application approach for each of the methods reviewed is evaluated and the most perspective research areas of GA application in sphere of information security

are established. The main aim of the analysis is to establish if there are any ready GA based solutions suitable for the fulfilment of the main objective.

Chapter 2 describes features of three selected modern malware types: Internet worms, which can be classified as the most aggressive malware type, relatively new mobile malware and rapidly evolving botnets, which may be considered as the biggest threat to modern information infrastructure. Understanding of malware propagation, survivability and other mechanisms is important for representation in a GA suitable format. Existing malware models are analysed in order to compare their features and efficiency with those proposed in the GA based malware risk evaluation and evolution forecasting model.

Chapter 3 presents malware risk level evaluation model and experimental investigation of its application to evaluation of Internet worm population stability threat after the satiation phase. Risk evaluation model is based on decision trees, composed out of the classified historical data and generated with the help of GA (GAtree software). The model tests on Internet worms with known population stability after the satiation phase are described.

Chapter 4 provides the description of malware evolution forecasting model, based on GA, that simulates the process of natural evolution to malware, which can be considered as a form of artificial life. Model is applied for three malware types: Internet worms, mobile malware and botnets, which were described previously. Evolution of two malware parameters: propagation techniques (for Internet worms, mobile malware, botnets) and survivability (for botnets) is being modelled. Model for Internet worm propagation technique evolution forecasting includes both friendly and hostile environment cases.

General conclusions as well as recommendations for further research summarises the present study. It is followed by an extensive list of 169 references and a list of 7 publications by the author on the topic of the dissertation.

General conclusions

1. According to the test results the principal correctness of the proposed genetic algorithm based malware risk evaluation model, using decision trees generated by the means of genetic algorithms for newly appearing malware risk evaluation, was approved. The proposed model can be recommended for automating the malware threat warning systems.
2. The modelling of perspective propagation strategies of Internet worms aiming to infect the highest number of computers in a limited period of time has shown the following evolution tendencies: Internet worms will tend to evolve to rather simple solutions, making use of a

popular OS platform, quick connectionless UDP based transfer mechanisms ("fire-and-forget" principal) and a combination of 4–5 exploits with high infection probability. Calculated fitness of the best strategy obtained during the experiment was equal to 1.18, which is 79 times higher than 0.015 of the most famous Code Red v.2 worm.

3. The modelling of perspective mobile malware propagation strategies, aiming to infect the highest number of computers in a limited period of time has shown that evolving mobile malware will tend to inclusion of several operating system platforms and propagation by WI-FI networks, compared to dominating nowadays MMS and Bluetooth. The forecasted propagation strategy tends not to be function overloaded. The fitness increased 1.7 times compared to a sample mobile virus.
4. Estimated evolution tendencies allow saying that consequences of future malware epidemic outbreaks can be more devastating than caused by modern malware, due to that novel methods, such as malware detection and blocking in network traffic, anomaly based detection mechanisms, network infrastructure load balancing, "bottleneck" prevention and others, should be developed and implemented to minimize the epidemic outbreak effect.

About the author

Nikolaj Goranin was born in Vilnius, on 26 of November 1981. First degree in Informatics Engineering, from Faculty of Fundamental Sciencies, Vilnius Gediminas Technical University (VGTU), 2004. Performed training at EU Joint Research Center IPSC CyberSecurity laboratory in 2004. Master of Science in Informatics Engineering, from Faculty of Fundamental Sciencies, VGTU, 2006. Has a job experience as a system administrator, teacher of informatics, FP6 and EU structural funds project coordinator and CISO. In 2006–2010 – PhD student of VGTU. At present – lecturer and junior scientific assistant at Department of Information Systems, Research Laboratory of Security of Information Technologies of VGTU.

Nikolaj GORANIN

GENETINIŲ ALGORITMŲ TAIKYMAS
INFORMACIJOS SAUGOS SISTEMOSE

Daktaro disertacijos santrauka
Technologijos mokslai, informatikos inžinerija (07T)

Nikolaj GORANIN

GENETIC ALGORITHM APPLICATION
IN INFORMATION SECURITY SYSTEMS

Summary of Doctoral Dissertation
Technological Sciences, Informatics Engineering (07T)

2010 04 30. 1,5 sp. l. Tiražas 70 egz.
Vilniaus Gedimino technikos universiteto
leidykla „Technika“,
Saulėtekio al. 11, 10223 Vilnius,
http://leidykla.vgtu.lt
Spausdino UAB „Biznio mašinų kompanija“,
J. Jasinskio g. 16a, 01112 Vilnius
http://www.bmk.lt