УДК 004.056:004.738

В. Ю. Михайлов, ä-р техн. наук, проф., Московский авиаöионный институт
(Наöионаёный иссёеäоватеёйский университет), e-mail: mihvj@yandex.ru,
В. Н. Гридин, ä-р техн. наук, проф.,
Центр инфорìаöионных техноёоãий в проектировании РАН, e-mail: info2@ditc.ras.ru,
Р. Б. Мазепа, канä. техн. наук, проф., Московский авиаöионный институт
(Наöионаёный иссёеäоватеёйский университет), e-mail: mrb402@mail.ru

Безопасное информационное взаимодействие. Проблемы и решения

Введение

Поä системìаìи инфорìаöионноãо взаиìоäейст-
вия (СИВ) буäеì пониìатü ёþбые инфорìаöионные
системìы, выпоёняþщие своþ заäа÷у путеì форìи-
рования и переäа÷и разнообразных сообщений
сёужебноãо (управёяþщеãо, увеäоìёяþщеãо) и öе-
ёевоãо (фактоãрафи÷ескоãо) типа.

Массовое испоёüзование инфорìаöионных тех-
ноёоãий во всех сферах äеятеёüности порожäает
необхоäиìостü созäания и испоёüзования разноо-
разных, призванных повыситü эффективностü этой
äеятеёüности СИВ. Лоãика развития СИВ такова,
÷то ее проãраììные коìпоненты не тоёüко интен-
сивно заìеняþт и äопоёняþт аппаратные коìпо-
ненты äёя äостижения высокой ãибкости и управ-
ёяеìости, обеспе÷иваþщие зна÷итеёüное проäёение
"жизненноãо öикёа" поäсистеì, но и становятся
основой СИВ как сёожных систеì. Отриöатеёüныì

Standard cell methodology is widely used for designing digital application specific integrated circuits (ASIC). A standard cell

is a group of interconnected transistors that provides a Boolean or storage function. Physical design is an important step in standard

cell based design flow, during this step geometrical representation of ASIC (layout) is obtained from geometrical representation of

standard cells. In this article some issues related to standard cell layout synthesis are considered. A routing algorithm for standard

cells that considers I/O ports accessibility, vertical cell porosity, blockages on higher metallization layers and layout regularity is

proposed. Routing models that takes constraints of 32 nm technology node into account are proposed as well. Presented algorithm

was utilized in an industrial tool for standard cell library synthesis. It showed acceptable runtime and high coverage of cells.

Keywords: layout synthesis, routing, standard cells

Рассмотрены вопросы безопасности систем информационного взаимодействия. Делается попытка системного анализа

основных проблем безопасности, в частности, причин и источников уязвимостей, способов проникновения в систему вре-

доносного программного обеспечения (ВПО) и методы борьбы с ним. Такой подход позволяет повысить эффективность ре-

шения задачи по сравнению с традиционным утилитарным стилем, использующим отдельные, слабосвязанные приемы, ме-

тоды и средства обеспечения информационной безопасности. В качестве главных объектов анализа предложены и исполь-

зованы логические каналы, среда исполнения и сервис среды исполнения. Отдельно рассмотрены также проблемы исполь-

зования существующих средств борьбы с ВПО, показана актуальность разработки комплексных средств борьбы с ВПО для

использования специалистами различной квалификации, в том числе и для некоммерческого применения.

Ключевые слова: информационные системы, информационное взаимодействие, логический канал, протокол, уязви-

мость, информационная безопасность

фактороì этоãо проöесса явёяется то, ÷то проãраìì-

ное обеспе÷ение по своей "инфорìаöионной" при-

роäе в зна÷итеёйно боёйøей степени, ÷еì обору-
äование поäвержено внеøниì, разруøитеёйныì
инфорìаöионныì возäействияì. Сёеäоватеёйно,
äостиãаеìая боёее высокая ãибкостü и управёяе-
ìостü СИВ распространяется и на неёеãаёйные ак-
тивные инфорìаöионные возäействия (напри÷ер,
неправиёйное испоёйзование открытых прото-
коёйных конструкöий), поäавёяþщие работу СИВ
иёи снижаþщие их эффективностü [1].

1. Общая характеристика
проблемы безопасности СИВ

Проектирование новых и ìоäернизаöия суще-
ствуþщих СИВ äоёжны у÷итыватü совреìеннуþ
опасностü инфорìаöионной среäы и тенäенöиþ к
постоянноìу нарастаниþ ее в бёижайøей пер-
спективе. Основныìи при÷инаìи стоёй неприят-
ноãо вывоäа явёяþтся:

- вынужäенное, в öеёях обеспе÷ения совìести-
ì о с т и, приìенение станäартных базовых про-
т о к оё о в, реаёизуþщих все уровни ìоäеёи OSI,
н о уже не отве÷аþщих в поёной ìере требова-
н и я ì безопасности;
- открытостü ёоãи÷еской среäы Интернет, в ос-
н о в н о ì обеспе÷иваþщей ãёобаёйное инфорìа-
ö и о н н о е взаиìоäействие;
- постоянный рост коёи÷ества и функöионаёйной
с ё о ж н о с т и СИВ, испоёйзуþщих оãрани÷енный
о б щ и й ресурс (напри÷ер, поёосу ÷астот), ÷то по-

рожäает разнообразные явёения уте÷ки инфорìаöии в физи÷еских канаёах переäа÷и äанных, а также возäеéствия на них внеøних естествен- н ы х возìущений и искусственных поìех;

 интенсивное развитие и приìенение беспро- в о ä н ы х техноёоãий инфорìаöионноãо взаиìо- ä е й с т в и я, испоёüзуþщих, в сиёу своей приро- ä ы, открытые физи÷еские раäиоканаёы;

 разнообразие проãраììно-аппаратных пёатфорì, ä о с т и ã а þщ и х совìестиìости с ёоãи÷еской сре- ä о й инфорìаöионноãо взаиìоäействия путеì и с п о ёü з о в а н и я ìножества, в основноì про- ãраììных, интерфейсов, явёяþщихся потенöи- а ёü н о äопоёнитеёüныìи исто÷никаìи уãроз;

 äоступностü простых äёя освоения и приìене- н и я высокоуровневых среäств проектирования п роãраììноãо обеспе÷ения (ПО), вовёекаþщих в проöесс разработки анаёизируþщих и вреäо- н о с н ы х проãраìì все боёее øирокий круã про- ãраììистов.

Разуìеется, в распоряжении разработ÷иков СИВ н а х о ä и т с я ìножество разнообразных ìетоäов, тех- н о ё о ã и й и прие ìов противоäействия возникаþ- щ и ì уãрозаì. Оäнако в сиёу разных при÷ин, в тоì ÷ и с ё е каäровоãо, произвоäственноãо и орãаниза- ö и о н н о ã о характера, они не в состоянии эффек- т и в н о и своевреìенно парироватü возникаþщие у ãрозы. Неёüзя забыватü, ÷то СИВ созäаþт и экс-

п ё у а т и руþт äёя реøения прикёааных öеёевых за-

ä а ÷, а не äёя борüбы с уãрозаìи. На наø взãёяä,

ì н о ж е с т в о этих при÷ин и порожäаеìых иìи про-

б ё е ììожно разбитü на сёеäуþщие катеãории.

1. Неопреäеёенностü реøаеìой заäа÷и безопас-

н о с т и СИВ.

В основноì эта катеãория иìеет отноøение к

п роектированиþ новых и сёожных, а сёеäоватеёйно,

ä о роãостоящих СИВ. К пробёеìаì äанноãо кёасса

о т н о с я т с я:

- неизвестностü потенöиаёüных уãроз, а сёеäова-

т е ёü н о, невозìожностü заёожитü в проект изу-

÷ е н н ы е и апробированные эффективные ìеха-

н и з ìы противоäействия;

- сёабая обоснованностü затрат на реøение по-

т е н ö и а ёü н ы х заäа÷ безопасности.

2. При÷ины, порожäаеìые конкурентной борü-

б о й и стреìёениеì быстро и äеøево парироватü уãрозы

б е з о п а с н о с т и СИВ.

Э т и при÷ины в основноì иìеþт отноøение к

ì о ä е рнизаöии (ìоäификаöии) существуþщих СИВ

и проäёениþ их жизненноãо öикёа. Вот основной

п е ре÷енü этих при÷ин, вкёþ÷аþщий порожäенные

и ì и пробёеìы:

- ìассовое привёе÷ение к реøениþ заäа÷ безо-

п а с н о с т и спеöиаёистов неäостато÷но высокой

к в а ё и ф и к а ö и и и (иёи) пёанирование неäопус-

т и ì о низких вреìенных ãраниö реøения заäа÷,

с ё е ä с т в и е ì ÷ еão явёяется их низкое ка÷ество;

 неэффективная практика противоäействия уãрозаì

ì е т о ä о ì сёабо контроёируеìоão "ёатания

ä ы р" иёи установки "запёаток" в существуþщеì

П О, саìих по себе явёяþщихся потенöиаёüныì

и с т о ÷ н и к о ì о ÷ ереäных "жу÷ков" (bugs) и воз-

ì о ж н о уязвиìостей;

 изобретение и приìенение "фирìенных" реøе-

н и й пробёеìы, за÷астуþ носящих характер рек-

ё а ì н ы х заявёений и ÷асто привоäящих к несо-

в ì е с т и ì о с т и инфорìаöионных протокоёов.

3. При÷ины систеìноão, проектноão характера,

с в я з а н н ы е с неäостато÷ныì вниìаниеì к то÷ности

и äетаёüности структурной проработки проекта,

в к ёþ ÷ а þщ е й:

– аäекватное описание преäìетной обёасти и

е е ãраниö (форìуёировку öееёей и заäа÷ СИВ);

– äекоìпозиöиþ систеìы и всех интерфейсов

н а функöионаёüноì, ёоãи÷ескоì и äруãих уровнях

п реäставёения;

– обоснование выбора принöипа инфорìаöион-

н о ã о взаиìоäействия коìпонентов систеìы (функ-

ö и о н а ёü н о связанное, синхронное иёи асинхрон-

н о е взаиìоäействие, взаиìоäействие посреäствоì

п о с ы ё к и сообщений (messaging) и äр.);

– резервирование и äруãие способы повыøения

н а ä е ж н о с т и, поìехо- и отказоустой÷ивости, ско-

рости восстановёения работоспособности систеìы;

– способы управёения режиìаìи функöиони-

рования поäсистеì, их состояниеì и повеäениеì.

Г ё а в н о й пробёеìой зäесü явёяется неäостато÷-

н о е ка÷ество проекта со сёабой аäаптаöией к из-

ì е н я þщ и ì с я усёовияì функöионирования и по-

т е нö и а ёü н ы ìуãрозаì.

4. При÷ины техноёоãи÷ескоãо характера, свя-

з а н н ы е с выбороì ìетоäов и вариантов реаёизаöии

(вопёощения) коìпонентов СИВ. К ниì ìоãут

б ы т ü отнесены:

- необоснованно ìаёое вниìание, уäеёяеìое корректности

и безопасности проãраììноãо коäа ПО;

- непоёная совìестиìостü реаёизаöий протоко-

ё о в инфорìаöионноãо взаиìоäействия на раз-

н ы х пёатфорìах;

- свойство новых разработок (в основноì ПО) к

з а иì с т в о в а н иþ старых и порожäениþ новых

о ø и б о к (bugs).

Резуёütатоì явёяется неэффективный, опасный и

п ё о х о поääаþщийся ìоäификаöии проãраììный коä

П О, оäной из ãёавных пробёеì котороãо явёяется

с ё а б а я защита от внеøних активных возäействий.

2. Потенциальные уязвимости СИВ

О ÷ е в и ä н о, ÷то пути и способы проникновения

и с с ё е ä у þщ е ã о (анаёизируþщеãо) и вреäоносноãо

П О (ВПО) в систему связаны с потенöиаёüныìи

у я з в иì о с т я ì и ее коìпонентов. На рисунке схеìа-

т и ÷ н о преäставёены направёения и öеёи атакуþщих

в о з äе й с т в и й на систеìу и ее ãёавные коìпоненты.

Л þ б ы е атакуþщие возäействия по существу экс-

п ё у а т и руþт ãёавнуþ уязвиìостü всех инфорìаöи-

о н н ы х систеì — еäинство инфорìаöионной среäы

и уровней совìестиìости ее с операöионныìи

с и с т е ì а ì и и их интерфейсныìи коìпонентаìи,

к о т о рые обеспе÷иваþтся, прежäе всеãо, протоко-

ё а ì и , реаёизуþщиìи ёоãи÷еские канаёы инфорìаöионноãо

в з а иì о äе й с т в и я . На рисунке эти кана-

ё ы отображены стреёкой, ёоãи÷ески соеäиняþщей

ä в а , возìожно разнороäных, эёеìента распреäе-

ё е н н о й инфорìаöионной систеìы.

2.1. Уязвимости логических каналов

Руковоäствуясü äанныì в работе [2] опреäеёе-

н и е ì ёоãи÷еских канаёов и соответствуþщих иì

п ротокоёов, рассìотриì основные исто÷ники их

у я з в иì о с т е й . Все ìноãообразие протокоёов распа-

äа е т с я на äва поäìножества: открытые (станäарт-

н ы е) и закрытые (коììер÷еские) протокоёы. Каж-

äо е из них иìеет свои äостоинства и неäостатки.

К äостоинстваì открытых протокоёов относятся:

- ãарантия совìестиìости инфорìаöионных про-

ö е с с о в в оãоворенных протокоёаìи ãраниöах;

- постоянство правиё инфорìаöионноãо взаиìо-

äе й с т в и я , ãарантируþщее ìассовое развитие на-

äе ж н ы х эёеìентов инфорìаöионных техноёоãий;

- известностü правиё всеì ёеãаёüныì у÷астникаì

и н ф о рìаöионноõо проöесса.

И з в е с т н о с т ü правиё инфорìаöионноõо взаиìо-

ä е й с т в и я иìеет и отриöатеёünуþ сторону, откры-

в а я возìожностü атакуþщиì осуществёятü öеёена-

п равёенные разруøитеёüные äействия. Друãиì

в а ж н ы ì неäостаткоì открытых протокоёов явёя-

е т с я их консервативностü, всёеäствие ÷еãо они не

о т в е ÷ а þ т растущеìу уровнþ "аãрессивности" ин-

ф о рìаöионной среäы.

Д о с т о и н с т в а закрытых протокоёов на первый

в з ãё я ä явёяþтся зеркаёüныì отображениеì неäостат-

к о в открытых протокоёов. Наприìер, неизвестностü

п равиё, казаёосü бы, äоёжна обеспе÷итü относитеёü-

н у þ безопасностü приìенения закрытых протоко-

ё о в . Оäнако не сёеäует забыватü, ÷то атакуþщие в

с и ё у ряäа известных при÷ин всеãäа иìеþт преиìу-

щ е с т в о наä защищаþщиìися и рано иёи позäно

в с к роþт первона÷аёüно неизвестный иì протокоё

и на÷нут испоёüзоватü еãо уязвиìости äо тоãо, как

разработ÷ик протокоёа оснастит еãо поёüзователёей

з а щ и т н о й "запёаткой". Сёеäоватеёüно, рассìотрен-

н а я особенностü закрытых протокоёов вряä ёи ìожет

рассìатриватüся как их äостоинство. Гибкостü пра-

в и ё закрытых протокоёов потенöиаёüно обеспе÷и-

в а е т возìожностü их аäаптаöии к растущеìу уровнþ

"аãрессивности" инфорìаöионной среäы. Оäнако эту

в о з ì о ж н о с т ü сёеäует еще реаёизоватü — эта особен-

н о с т ü закрытых протокоёов ìожет статü äостоинст-

в о ì ёиøü в сёу÷ае наäежноão и постоянноão их со-

п ровожäения разработ÷икоì. Практика показывает,

÷ т о бес÷исёенные пакеты обновёения (service packs),

"запёатки" (patches), а также äруãие не сёиøкоì

в разуìитеёüные проãраììные среäства (updates,

bugfixes и т. ä.) ÷ерез некоторое вреìя все же не

с п равёяþтся с наãрузкой и их заìеняþт новой раз-

работкой. Иныìи сёоваìи, рассìотренное äосто-

и н с т в о ёиøü вреìенное.

С реäи явных неäостатков закрытых протокоёов

о с о б о выäеёяþтся сёеäуþщие:

- сиёüная зависиìостü разработ÷иков ПО от не-

и з в е с т н ы х иì ìоäификаöий протокоёов;

- неизвестный, неконтроёируеìый и ÷асто просто

ä е к ё а рируеìый уровенü защищенности поёüзо-

С реда и разрушительные воздействия ватеёей.

В наибоёüøей степени и ранüøе всех остаёüных

рассìотренные ёоãи÷еские канаёы и соответствуþ-

щ и е иì протокоёы испоёüзуþт сёеäуþщие обще-

распространенные сетевые Internet-приёожения:

- Web-браузеры и Web-серверы;
- Ftp-кёиенты и серверы;
- по÷товые кёиенты и серверы;
- кёиенты и серверы систеì ìãновенноão обìена

с о о б щ е н и я ì и (IM);

- кёиенты пиринãовых сетей (P2P);
- кёиенты и серверы баз äанных.

Э т и приёожения, явёяясü, по сути, "то÷каìи вхо-
ä а " в уäаёеннуþ систему, первыìи приниìаþт на
с е б я атакуþщие возäействия. Оäнако эти приёо-
ж е н и я явёяþтся высокоуровневыìи и их работа
б а з и руется на сетевых сёужбах и протокоёах. Наи-
б о ё е е опасныìи из них явёяþтся Net Logon, DNS,
DHCP, WINS, Telnet, RPC (NetDDE), Proxy-сер-
в е ры, RDS, Terminal Services, Remote Registry Service,
NetBios, TCP/IP и äр.

2.2. Уязвимости среды исполнения

О б ы ÷ н о поä среäой испоёнения пониìается опе-
раöионная системà и преäоставёяеìый еþ про-
ãраììныì коìпонентаì так называеìый системный
с е рвис. На рисунке среäа испоёнения показана в ви-
ä е стреёки, соеäиняþщей уровенü операöионной
с и с т е ìы с уровнеì приёожений. Уязвиìости среäы
и с п о ё н е н и я порожäаþтся äвуìя ее особенностяìи:
с т руктурной и функöионаёüной.

С т руктурная особенностü среäы испоёнения
с о с т о и т в øирокоì äиапазоне уровней ìоäеёи OSI,
н а которых работаþт коìпоненты операöионной
с и с т е ìы : от MAC-уровня äо прикёääноãо. В своей
работе эти коìпоненты созäаþт ìножество параёёеёüных
п роãраììных потоков, испоёüзуþщих оäин
и тот же ресурс паìяти, ÷то при пёохой синхрони-
з а ö и и (оøибки сёу÷аþтся всеãäа) созäает опас-
н о с т ü проникновения на уровенü приёожений ви-
русов и äруãих зёовреäных проãраìì. Сёеäствия

т а к о ã о проникновения сёеäуþщие:

 изìенение режиìов работы коìпонентов ОС,

в п ё о т ü äо захвата вирусаìи (зёовреäныìи про-

ãраììаìи) контроёя наä ней;

 неконтроёируеìые обёасти паìяти ìоãут бытü

п роанаёизированы "øпионаìи" на преäìет вскры-

т и я проãраììноãо коäа и ìетоäов øифрования;

 конфёикты ìежäу потокаìи, которые созäаþт

у с ё о в и я äёя сбоев и отказов проãраììных коì-

п о н е н т о в .

Ф у н к ö и о н а ёü н ы е особенности среäы испоёнения

в ы ражаþтся в виäе øирокоãо набора разёи÷ноãо

у ровня усёуã, преäоставёяеìых ОС проãраììаì и

реаёизованных на разёи÷ных языках проãраììи-

рования с испоёüзованиеì разнообразных техно-

ё о ã и й . Так как существуþщие ОС не оãрани÷иваþт

и с п о ёü з о в а н и е как разёи÷ных типов сервисных коì-

п о н е н т о в ОС, так и техноёоãий разработки ПО, то

п о я в ё я е т с я опасностü несовìестиìости при взаи-

ì о ä е й с т в и и ОС с прикёааныìи проãраììаìи. Дос-

т и ж е н и е совìестиìости требует äопоёнитеёüных

п реобразований, снижаþщих быстроäействие СИВ.

Разнообразие высокоуровневых техноёоãий, ис-

п о ёü з у е ì ы х ПО, привоäит к äубёированиþ опера-

ö и й на низкоì уровне и, сёеäоватеёüно, к зависи-

ì о с т и оøибок при проãраììировании. Основой

к оì п о н е н т н о ã о проектирования, как известно, яв-

ё я е т с я боãатый выбор ãотовых коìпонентов и ìас-

с о в о е их испоёизование в разработках ПО. Выбор

ã о т о в ы х коìпонентов с у÷етоì разнообразия ис-

п о ёü з о в а н н ы х в них языков и техноёоãий проãраììирования

н е всеãäа отве÷ает аäекватноìу их взаи-

ì о ä е й с т в и þ äруã с äруãоì и с äруãиì ПО.

О с н о в н ыì и коìпонентаìи, составёяþщиìи

с реäу испоёнения, явёяþтся сёеäуþщие приёоже-

н и я и объекты ёокаёйноãо äействия:

- интерпретируþщие приёожения и их объекты (текстовые и табёи÷ные проöессоры), вкёþ÷аþщие к ё и е н т с к и й коä на сöенарных языках Java, JavaScript, VB Script, PHP и äр.;
- коìанäные и сёужебные файёы операöионных с и с т еì: com-, bat-, inf-файёы, WSH-приёожения;
- Autorun и кёþ÷и реестра: HKLM\SYSTEM\CurrentControlSet\Services\;
- файёовая систеìа;
- äрайверы устройств;
- коìпоненты уровня яäра ОС.

2.3. Уязвимости сервиса среды исполнения

П о ä сервисоì среäы испоёнения пониìается

п роãраììный сервис, преäоставёяеìый операöион-

н о й систеìой и äруãиìи прикёääныìи сёужбаìи

п роãраììныì коìпонентаì äёя реаёизаöии ìеж-

п роãраììноãо (ìежкоìпонентноãо) взаиìоäействия.

Н а рисунке сервис среäы испоёнения показан в

в и ä е стреёки, соеäиняþщей коìпоненты проãраìì-

н о ã о обеспе÷ения. Особенностüþ äанноãо сервиса

я в ё я е т с я испоёизование äёя этой öееи øирокоãо
н а б о ра высокоуровневых техноёоãий, ÷то в совокуп-
н о с т и с боёïøиì разнообразиеì техноёоãий проек-
т и рования ПО способствует "разìножениþ" кон-
ф ё и к т о в как ìежäу разёи÷ныìи коìпонентаìи ПО,
т а к и ìежäу коìпонентаìи ПО, с оäной стороны, и
с и с т е ì н ы ì сервисоì, с äруãой стороны. Гёавныì от-
ё и ÷ и е ì уязвиìостей äанноãо типа от рассìотренных
в ы ø е явёяется появёение новоãо их исто÷ника: при-
к ё а ä н о ã о сервиса, расøиряþщеãо систеìный сервис.
О ÷ е в и ä н о , ÷то на этоì уровне рассìотрения ис-
п о ёü з у þ т с я наибоёее разнообразные коìпоненты
П О и протекаþт наиìенее контроёируеìые проöес-
с ы их взаиìоäействия. Поэтоìу несìотря на то ÷то
ä а н н ы й уровенü изоёирован от опасной инфорìаöи-
о н н о й среäы, проникøие сфäа вреäоносные про-
ãраììы иìеþт в своеì распоряжении øирокие воз-
ì о ж н о с т и по экспёуатаöии появивøихся уязвиìо-
с т е й . Наконеö, прикёääное ПО проектируется и от-
ё а ж и в а е т с я в усёовиях, отёи÷аþщихся от рабо÷их, —
в операöионной среäе, ãäе ÷аще всеãо нет усёовий
äё я возникновения поäобных реаёüных уязвиìостей.

И з изёоженноãо вытекаþт сёеäуþщие вывоäы:

- äостижение совìестиìости требует от проãраììи-
с т о в хороøеãо знания структуры ОС, так как при-
к ё а ä н о е ПО возäействует на систеìный сервис;
- разнообразие высокоуровневых техноёоãий

привоäит к äубёированиþ операöий на низкоì

уровне и, сёеäоватеёüно, к зависиìости оøибок

при проãраììировании;

 несоответствие версий систеìноãо сервиса, ис-

поёüзуеìоãо при разработке и экспёуатаöии

ПО, привоäит к сбояì и отказаì, явёяясü äо-

поёнитеёüныì исто÷никоì уязвиìостей СИВ.

3. Условия проникновения,

методы обнаружения и борьбы с ВПО

3.1. Условия проникновения ВПО

Провеäенный выøе анаёиз исто÷ников уязви-

ìостей позвоёяет сформìуёироватü ãёавные усёо-

вия проникновения и активизаöии ВПО в сёеäуþ-

щеì виäе:

 наёи÷ие сетевых кёиентов и сёужб и работа в сети;

 оøибки ìанäатноãо äоступа (работа поä аäìи-

нистративныì аккаунтоì);

 оøибки äискреöионноãо äоступа (äоступ к объ-

ектаì);

 коёи÷ество, структура активных проöессов и их

состояние;

 испоёüзование режиìа автообновёения ПО;

 неправиёüные настройки ìежсетевоãо экрана

(Firewall), антивирусноãо и äиаãности÷ескоãо ПО;

 небезопасные настройки приёожений и сёужб;

 наёи÷ие и настройка отёаä÷иков;

 оøибки проектирования (ёиøние связи ìежäу

коìпонентаìи ПО и операöионной среäой,

а также ìежäу отäеёйныìи коìпонентаìи ПО);

 оøибки проãраììирования (прежäе всеãо оøиб-

к и работы с паìятüþ).

3.2. Методы обнаружения ВПО

В с е ìетоäы обнаружения ВПО разäеёяþт на три

т и п а в зависиìости от испоёüзуеìой иìи техноёо-

ã и и обнаружения: обнаружение на этапе заãрузки,

о б н а ружение в проöессе работы ОС и обнаружение

п ри работе ОС поä управёениеì ãипервизора. Не-

о б х о ä и ì о с т ü испоёüзования ìетоäов обнаружения

п е рвоãо типа обусёовёена способностüþ ВПО (в ÷а-

с т н о с т и Rootkit [3]) "прятатüся" посёе заãрузки ОС

т а к , ÷то ìетоäы второãо типа просто не в состоя-

н и и обнаружитü. Ясно, ÷то такие ìетоäы явёяþтся

с а ìы ì и сёожныìи и саìи преäставёяþт собой не-

к о т о рое "супер ВПО", способное "обоãнатü" ВПО в

п роöессе заãрузки ОС и "поäсìотретü" такиì обра-

з о ì проöесс заãрузки остаёйных коìпонентов ОС.

О ä н и ì из неìноãих эффективных среäств обна-

ружения ВПО первоãо типа явёяется пакет RegRun

ф и рìы Greatis, который с поìощüþ спеöиаёйноãо

äрайвера Partizan реøает сёеäуþщуþ заäа÷у: иìея

п о ё н ы й äоступ к объектаì ОС, выявёяет опасные

ф а й ё ы и соответствуþщие иì кёþ÷и реестра на ос-

н о в а н и и базы äанных известноãо ВПО (Greatis Application

Database).

К основныì ìетоäаì обнаружения ВПО второ-

ã о типа относятся:

 поиск проãраìì, приìеняþщих ìеханизìы Rootkit;

 анаёиз запущенных проöессов;

 анаёиз проöесса и режиìов автозапуска проãраìì;

 поиск опасных и новых файёов в систеìных ка-

т а ё о ã а х на äиске (катаёоãи Windows, System32, Drivers, Security Storage и äр.);

 анаёиз файёовых ìенеäжеров и ìоäуёей расøи-

рения Internet Explorer;

 анаёиз файёа hosts.

Я ркиì приìероì реаёизаöии ìетоäов третüеãо

т и п а явёяется проãраììное среäство новоãо кёасса Hypersight Rootkit Detector. В настоящий ìоìент это

е äи н с т в е н н а я проãраììа, способная контроёироватü

ö е ё о с т н о с т ü яäра ОС, при этоì она работает "про-

з ра÷но" äёя ОС и всех проãраìì, запущенных в ней.

3.3. Проблемы использования существующих средств борьбы с ВПО

П е ре÷исёиì ãёавные пробёеìы рассìотренных и äруãих проãраììных среäств борüбы с ВПО.

1. Сёожностü обоснования выбора и испоёüзо-

в а н и я конкретноãо инструìентария борüбы с ВПО.

П о ёü з о в а т е ёü äоёжен обёаäатü высокой кваёи-

ф и к а ö и е й в обёасти инфорìаöионной безопасно-

с т и и иìетü ÷еткое преäставёение о назна÷ении и

х а рактеристиках объектов защиты, назна÷ении и

х а рактеристиках среäств защиты.

2. Сёожностü интерпретаöии резуёüтатов рабо-

т ы среäств борüбы с ВПО и посёеäуþщих äействий

п о ёü з о в а т е ё я.

Ряä среäств борüбы в итоãе ãенерирует от÷ет о

п реäпоёожитеёüно найäенноì ВПО, а выбор ääёüней-

ø и х äействий возёаãается на поёüзоватеёя. В ÷астно-

с т и, поёüзоватеёü саì реøает, ÷то äеёатü на этапе сёе-

ä у þщ е й заãрузки систеìы. В сёу÷ае "нейтраёизаöии"

В П О поёüзоватеёü ìожет тоёüко äоверитüся резуёüта-

т а ì работы испоёüзуеìых среäств борüбы с ВПО.

3. Работа проãраìì̈ных среäств обнаружения

В П О по принöипу "÷ерноãо ящика".

С к рытостü ìетоäов работы конкретноãо среäст-

в а борüбы с ВПО, техноёоãий разработки и саìоãо

п роãраìì̈ноãо коäа препятствует их оперативноìу

в н е äрениþ.

4. Боёü̈инство среäств борüбы с ВПО явёяþт-

с я коìì̈ер÷ескиìи.

С ё е ä у е т, оäнако, отìетитü, ÷то ряä произвоäи-

т е ё е й (напрӥер, упоìянутые выøе Greatis, Лабо-

ратория Касперскоãо) сеãоäня преäоставёяет на

рынок беспёатные версии своих проãраìì̈ных

с реäств, нескоёüко боёее "ёеãкие" по сравнениþ с

и х поёноöенныìи коìì̈ер÷ескиìи анаёоãаìи.

З а к л ю ч е н и е

О ä н и ì из ãёавных резуёüтатов провеäенноãо

а н а ё и з а явёяется вывоä о öеёесообразности разра-

ÈÍÔÎÐÌÀÖÈÎÍÍÛÅ ÒÅÕÍÎËÎÃÈÈ, ¹ 10, 2014 77

б о т к и еäиной ìетоäики и соответствуþщеãо набо-

ра инструìентаёиных среäств борёбы с ВПО. Гёав-

н ы е составёяþщие обоснования äостижиìости та-

к о й öеёи выãёяäят так.

1. Открытостü ОС.

Б о ёüø и н с т в о ОС — коììер÷еские. Оäнако ар-

х и т е к т у ра существуþщих операöионных систеì

(Windows, Unix/Linux, Mac OS), вкёþ÷ая ìобиёü-

н ы е пёатфорìы, известна.

2. Пробёеìа иссёеäования "траекторий" внеäре-

н и я ВПО.

Н а х о жä е н и е всех возìожных то÷ек проникно-

в е н и я ВПО в систеìу (сì. рисунок) впоёне реаёü-

н о . Оäнако требуется обоснование отсутствия äру-

ã и х (необнаруженных) то÷ек вхоäа.

3. Пробёеìа иссёеäования повеäения ВПО.

Б а з о й проäуктивной работы ёþбоão ВПО явёя-

е т с я ìножество функöий, бибёиотек и äруãих объ-

е к т о в среäы испоёнения. Опреäеёение этоão ìно-

ж е с т в а , факта и посёеäоватеёüности (поряäка) вы-

з о в а функöий позвоёит äостато÷но то÷но выäеёитü

В П О на фоне ёеãаёüных проöессов.