Таблица 1 – Результаты наблюдений

Вид отказа	Количество отказов		
	Intel Pentium E5700 (2 шт.)	Intel Celeron E3400(5 шт)	Всего
Отказ работы технического устройства в связи с выработкой ресурса, шт (стр. 1)	2	0	2
Отказ работы технического устройства в связи с браком (ранний отказ), шт (стр. 2)	0	2	2
Отказ работы технического устройства в связи с неправильным обращением пользователя, шт (стр. 3)	3	4	7
Отказ работы печатающего устройства, шт (стр. 4)	2	2	4
Отказ функционирования ПО в связи с проникновением вредоносных программ, шт (стр. 5)	0	1	1
Итого отказов, шт (стр. 6 = стр. 1 + стр. 2 + стр. 3 + стр. 4 + стр. 5)	7	9	16
Суммарная длительность ожидания осмотра при отказе, час (стр. 7)	0,8	2,3	3,1
Суммарная длительность осмотра и ремонта при отказе, час (стр. 8)	0,9	2,1	3,0
Суммарная длительность восстановления работоспособного состояния при отказе, час (стр. 9 = стр. 7 + стр. 8)	1,7	4,4	6,1
Суммарная наработка, час (стр. 10)	1029	2562	3591
Техническое обслуживание, шт (стр. 11)	2	3	5
Средняя наработка на отказ, час (стр. 12)	147	285	
Среднее время восстановления работоспособ-ного состояния, час (стр. 13)	0,243	0,489	
Суммарная длительность технического обслуживания, час (стр. 14)	1,3	3,8	5,1
Коэффициент готовности	0,99835	0,99829	

Выводы: наблюдения за компьютерами такого класса в таком объёме проводились в республике впервые. Их результаты продолжают обрабатываться.

Список использованных источников:

1. Бахтизин В.В., Лукашик О.А., Сечко Г.В. Формы для сбора и обработки результатов наблюдений за работой компьютеров // Тез. докл. 5-й белорусско-российской НТК “Технические средства защиты информации”, Нарочь, 28 мая-1 июня 2007 года). – Мн.: БГУИР, 2007. – С. 37.

МЕРОПРИЯТИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ВИРТУАЛЬНЫХ СИСТЕМАХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Шелков А. С.

Бойправ О. В.– м-р техн. наук, ассистент

На современном этапе развития информационных технологий наблюдается бурный рост рынка технологий виртуализации, в частности, виртуальных сред. Использование последних позволяет создавать компьютерные системы с гибкой инфраструктурой и повышенной надёжностью. Однако применение виртуальных сред порождает новые виды угроз информационной безопасности, которые следует предотвращать.

Виртуальная среда представляет собой совокупность виртуальных машин, гипервизоров и систем управления виртуальной инфраструктурой. В качестве виртуальной машины выступает программа, которая эмулирует настоящий физический компьютер. Гипервизор представляет собой программное обеспечение, позволяющее осуществить одновременный запуск нескольких операционных систем на одном компьютере и обеспечивающее взаимодействие между аппаратными ресурсами и виртуальными машинами. Система управления виртуальной инфраструктурой – это программное обеспечение, управляющее несколькими гипервизорами и виртуальными машинами, которые на них установлены.

Виртуальная среда характеризуется рядом особенностей, основные из которых заключаются в том, что:

– сетевые коммуникации между виртуальными машинами проходят через виртуальный коммутатор гипервизора без выхода трафика за его пределы;

– виртуальных машина представляет собой набор файлов;

– администрирование виртуальной среды является задачей повышенной сложности.

Анализируя структуру виртуальных сред и её особенности, можно определить направления новых видов угроз информационной безопасности и разработать методику борьбы с ними. По отношению к виртуальным средам могут быть реализованы следующие угрозы:

– атака на гипервизор либо из физической сети, либо с виртуальной машины;

– атака на средства администрирования виртуальной инфраструктуры;

– атака на виртуальную машину с другой виртуальной машины.

В комплексе мер, направленных на защиту виртуальных сред, наиболее значимое место должно занимать компетентное администрирование. Оно позволяет существенно повысить уровень защищённости среды. Наряду с администрированием должны реализовываться и иные меры, которые включают в себя:

– применение традиционных методов защиты, которые используются на реальных машинах;

– применение новых методов, основанных на использовании отдельной виртуальной машины или машин, специализированных на обеспечение информационной безопасности всей виртуальной среды.

Преимущество использования специализированных виртуальных машин состоит в том, что они централизуют защитные средства виртуальной среды, упрощая контроль над ними, и способствуют снижению потребления аппаратных ресурсов.

Причём виртуальные машины защиты можно использовать в качестве:

– антивирусного программного обеспечения (например, Kaspersky Security для виртуальных сред);

– анализатора виртуального сетевого трафика (для этого используются виртуальные коммутаторы, например, Cisco Nexus серии1000V);

– виртуальных межсетевых экранов

Таким образом, задача обеспечения информационной безопасности виртуальных систем на сегодняшний день должна являться одной из наиболее актуальных для компаний-разработчиков средств виртуализации.

ПРОЕКТ ПРОГРАММНОГО СИМУЛЯТОРА САМООРГАНИЗУЮЩЕЙСЯ ЭКОНОМИЧЕСКОЙ СИСТЕМЫ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Шманай А. С.

Калугина М. А. – канд. физ.-мат. наук, доцент

Программные симуляторы самоорганизующихся систем находят себе практическое применение в целой группе отраслей человеческого знания и позволяют решать задачи по оптимизации и моделированию процессов, используются в качестве инструментов исследований и для развлекательных целей. Целью программных средств данного класса является построение динамической модели самоорганизующейся системы определённого рода.

Самоорганизация — процесс упорядочения элементов одного уровня в системе за счёт внутренних факторов и появления единиц следующего качественного уровня [1]. Самоорганизующаяся система – это фундаментальное понятие, которым оперирует множество наук и исследования в области самоорганизующихся систем могут принести пользу во многих направлениях человеческой деятельности. В пользу данного утверждения говорит то, сколько существует исследований и уникальных разработок напрямую связанных с вопросами самоорганизации. В частности, в 2013 году группой инженеров из Калифорнийского технологического института был создан кластер из компьютерных чипов, способный восстанавливать свою работоспособность после физических повреждений. Результаты научного исследования опубликованы в мартовском номере журнала “IEEE Transactions on Microwave Theory and Techniques”. Предварительная статья под названием “A Fully-Integrated Self-Healing Power Amplifier” получила награду как лучшая статья на симпозиуме 2012 “IEEE Radio Frequency Integrated Circuits”. Помимо этого, в 2013 году учёные Кристос Саккелариу и Питер Бентли из Университетского колледжа Лондона, создали прототип самовосстанавливающейся компьютерной системы, которая основана на принципах работы живых организмов. Разработкой Саккелариу и Бентли уже заинтересовались руководители европейского проекта “Human Brain Project” по созданию гигантского симулятора человеческого мозга. Евросоюз одобрил финансирование этого проекта в размере 1,19 миллиарда евро, и сейчас организаторы начали подготовительную фазу, в процессе которой нужно определить наиболее подходящую аппаратную платформу для эмуляции нейронов человеческого мозга.

По принципу построения симуляции живые системы можно разделить на следующие виды [2]: