ВВЕДЕНИЕ

Стремительное развитие технологий виртуализации и создание сред облачных вычислений формирует новые источники угроз, которые необходимо учитывать при обеспечении кибербезопасности современных компьютерных систем и сервисов. При этом динамический характер процессов информационного взаимодействия существенно затрудняет возможности оперативной оценки рисков нарушения конфиденциальности, целостности и доступности программных и инфраструктурных ресурсов, предоставляемых в режиме удаленного доступа. Традиционные средства обеспечения информационной безопасности (*средства разграничения доступа, межсетевые экраны, системы обнаружения вторжений и т.п.)*контролируют только те информационные потоки, которые проходят по каналам, предназначенным для их передачи, поэтому угрозы, реализуемые посредством скрытых каналов передачи информации, с их помошью не могут быть блокированы. В этих условиях важное значение приобретают технологии защиты от угроз, которые формируются с использованием скрытых каналов информационного воздействия или внутри периметра безопасности корпоративной компьютерной сети. Защита от таких деструктивных воздействий должна осуществляться на уровне процессов управления системными вызовами или контроля недекларированных возможностей (НДВ) прикладного программного обеспечения (ПО), что требует создания новых моделей и методов противодействия попыткам внешних и внутренних пользователей изменить состояние защищенности информационных ресурсов среды облачных вычислений.

Актуальность решения этой важной научно-технической задачи отмечается многими российскими и зарубежными учѐными, в том числе В. А. Курбатовым, П. Д. Зегждой, А.А.Грушо, В.Ю. Скибой, Н.А. Гайдамакиным, А.А. Гладких, В.С. Заборовским, С. Воглом, Р. Сэйлером, Ф. Мортинелли, Дж. Рутковской и др. В работах перечисленных авторов большое внимание уделяется разработке средств защиты информации, в которых учитываются особенности технологий виртуализации и возможности современных аппаратно-программных компонент вычислительных систем, непосредственно влияющие на защищенность системных и прикладных процессов.

В отечественных и зарубежных научных публикациях описываются лишь базовые подходы контроля сигнальных событий в контуре распределенных вычислительных систем [5 - 20] . В современных научных школах США и Великобритании (на основании открытых публикаций) по исследованию вирусного кода и изучению методов обнаружения программных «закладок» используется классический подход - спецификация базовых информационных сервисов операционных систем (ОС), маркерные сигнатуры, динамический анализ исполняемого кода на уровне KOS (KernelObjectSpecification) [21 - 63].

Данные исследования не затрагивают рассмотрение проблемы неявных механизмов контроля ресурсов операционной системы и принципов «*невидимости*». Классические подходы и методы с использованием упомянутой выше спецификации KOSне позволяют обнаруживать новые образцы вредоносного ПО, использующего технологии DKOM (DirectKernelObjectManipulation) и VICE(VirtualICE) [69 - 74].

обмена, нарушение целостности и доступности ресурсов, блокирование доступа и навязывание ложной информации, является актуальной научно-технической задачей, решению которой посвящена данная диссертационная работа.

Целью исследования является разработка средств противодействия скрытым угрозам информационной безопасности в среде облачных вычислений, учитывающих архитектуру гипервизора и особенности современных технологий виртуализации аппаратных ресурсов.

Для достижения поставленной цели в диссертационной работе были решены следующие задачи:

1. Разработана модель скрытых угроз информационной безопасности, учитывающая контекст выполнения операций информационного взаимодействия в среде облачных вычислений.
2. Разработана модель операций, выполняемых над данными при их обработке в среде облачных вычислений, позволяющая формализовать описание информационных процессов в виде мультиграфа транзакций.
3. Разработан метод противодействия скрытым угрозам, основанный на контроле запросов на выделение ресурсов в соответствие с оценкой безопасности выполняемых транзакций.
4. Разработан алгоритм предикативной идентификации угроз, возникающих для подсистем гипервизора при реализации запросов гостевых ОС на выделение информационных ресурсов.
5. Создан опытный образец программного обеспечения под названием «Альфа - монитор» и проведена его успешная апробация в среде облачных вычислений.

Методы исследования: для решения сформулированных задач использовался аппарат теории графов, теории алгоритмов, теории вероятностей, методы защиты информации и компьютерного реверс-инжиниринга.

Объект исследования: скрытые угрозы информационной безопасности в среде облачных вычислений.

Предмет исследования: модели, методы и алгоритмы обнаружения скрытых угроз на уровне гипервизора среды облачных вычислений и гостевых операционных систем виртуальных машин (ВМ).