На правах рукописи

Никольский Алексей Валерьевич

ЗАЩИТА ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ ОТ АТАК НА СРЕДСТВА ВИРТУАЛИЗАЦИИ

Специальность 05.13.19

Методы и системы защиты информации, информационная безопасность

Автореферат диссертации на соискание ученой степени кандидата технических наук

Санкт-Петербург – 2013

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего профессионального образования «Санкт-Петербургский государственный политехнический университет»

Научный руководитель:

Зегжда Дмитрий Петрович,
доктор технических наук, профессор

Официальные оппоненты:

Баранов Александр Павлович,
доктор физико-математических наук,
профессор, зав. каф. информационной безопасности, НИУ ВШЭ

Красов Андрей Владимирович,
кандидат технических наук, профессор кафедры ИБТС, ГОУ ВПО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»

Ведущая организация: ФГОУ ВПО «Петербургский государственный университет путей сообщения»

Защита состоится « » декабря 2013 г. в часов на заседании диссертационного совета Д 212.229.27 при ФГБОУ ВПО «Санкт-Петербургский государственный политехнический университет» (по адресу 195251, Санкт-Петербург, ул. Политехническая, д.29/1, ауд. 175 главного здания)

С диссертационной работой можно ознакомиться в Фундаментальной библиотеке ФГБОУ ВПО «Санкт-Петербургский государственный политехнический университет».

Автореферат разослан « » ноября 2013г.

Ученый секретарь
диссертационного совета

Платонов Владимир Владимирович

Общая характеристика работы

Актуальность темы исследования. В настоящее время облачные технологии интенсивно развиваются и внедряются во многие коммерческие компании и государственные организации, поэтому обеспечение информационной безопасности систем облачных вычислений (СиОВ) является критически важной задачей. Как правило, защита СиОВ обеспечивается с помощью межсетевых экранов, криптографических средств и других механизмов, не учитывающих возможности внутреннего нарушителя.

Основой для построения систем облачных вычислений являются средства виртуализации (гипервизоры), которые обеспечивают работу виртуальных машин (ВМ) в СиОВ. Нарушители, имеющие доступ к ВМ, могут совершать атаки на средства виртуализации путем эксплуатации уязвимостей (таких как, CVE-2011-1751 в KVM и CVE-2012-0217 в Xen), список которых пополняется каждый год. Пользователи обладают разными правами доступа к ресурсам СиОВ, однако гипервизоры назначают всем ВМ одинаковые привилегии, причем эти привилегии чаще всего избыточны. Кроме того, гипервизоры обладают исключительными привилегиями во внутренней инфраструктуре СиОВ, что открывает нарушителю, в случае успешной атаки на гипервизор, доступ практически ко всем информационным ресурсам СиОВ. Следовательно, для обеспечения безопасности облачных вычислений необходимо контролировать привилегии не только пользователя, но и компонентов гипервизора, обрабатывающих запросы ВМ, а также процесс их обработки во внутренней инфраструктуре СиОВ.

Из вышеизложенного следует актуальность постановки задачи по разработке методов построения гипервизоров для облачных вычислений, позволяющих нейтрализовать атаки на средства виртуализации, обусловленные успешной эксплуатацией уязвимостей. Актуальность подтверждается и приказом ФСТЭК № 21 от 18 февраля 2013 г.

Тема работы соответствует пунктам 6 и 13 паспорта специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Степень разработанности темы исследования. Известными отечественными и зарубежными учеными, занимающимися проблемами безопасности облачных вычислений и моделированием безопасности

распределенных систем, являются В.Е. Козюра, В.А. Курбатов, В.И. Будзко, В.С. Заборовский, Ф. Мартинелли, Р.Б. Ли, Р. Сэйлер и С. Вогл.

В современных работах защиту гипервизоров предлагается обеспечить с помощью средств мандатного контроля доступа (проект sHype) или криптографических средств (проект Terra). Таким образом, в этих работах решаются задачи изоляции ВМ друг от друга и защиты ВМ от воздействий со стороны гипервизоров, но не учитываются особенности атак на средства виртуализации.

Целью работы является защита систем облачных вычислений от атак, направленных на средства виртуализации, с использованием мультидоменного гипервизора, обеспечивающего монотонное убывание привилегий в ходе обработки запросов пользователей. Для достижения поставленной цели в работе решались следующие задачи:

1. Разработка модели угроз для гипервизоров в системах облачных вычислений, учитывающей атаки на средства виртуализации.
2. Создание формальной модели атак на средства виртуализации и разработка оценки степени устойчивости гипервизоров к атакам.
3. Разработка архитектуры мультидоменного гипервизора, обеспечивающего защиту от атак на средства виртуализации.
4. Построение формальной модели обработки запросов в СиОВ.
5. Разработка методики обеспечения безопасной обработки запросов в СиОВ на основе принципа наименьших привилегий путем монотонного убывания привилегий в ходе обработки запросов.
6. Создание опытного образца мультидоменного гипервизора и его апробация в СиОВ.

Научная новизна диссертационной работы состоит в следующем:

– обоснована необходимость распределения компонентов гипервизора по доменам с различными привилегиями, что обеспечивает защиту от атак на средства виртуализации, в соответствии с разработанной формальной моделью атаки;

– предложена оценка степени устойчивости гипервизоров к атакам;

– впервые предложена архитектура мультидоменного гипервизора, обеспечивающая защиту от атак на средства виртуализации;

– разработана формальная модель безопасной обработки запросов, позволившая сформулировать принцип монотонного убывания привилегий;

– разработана методика обеспечения монотонности убывания привилегий при обработке запросов.

Практическая значимость результатов определяется возможностью использования предложенных моделей и методики для сравнительной оценки устойчивости гипервизоров различной архитектуры к атакам внутреннего нарушителя и для практической реализации мультидоменного гипервизора, обеспечивающего защиту СиОВ от атак на средства виртуализации.

Результаты работы представляют практическую ценность для разработчиков защищенных систем облачных вычислений и средств виртуализации.

Внедрение результатов исследований. Предложенный подход к построению гипервизоров для СиОВ, защищенных от атак на средства виртуализации, нашёл применение при разработке методов работы программно-конфигурируемых сетей в рамках НИР «Анализ и разработка методов и алгоритмов управления сетевыми ресурсами и потоками данных в программно-конфигурируемых компьютерных сетях» (шифр «2012-1.4-07-514-0021-025») по государственному контракту от 14 июня 2013 г. № 07.514.11.4151.

Предложенная модель атаки на средства виртуализации и методика практического использования мультидоменного гипервизора использовались в рамках НИОКР «Управление-Контроль» ООО «РОСРЕЧИНФОКОМ»; оценка степени устойчивости гипервизора к атакам и архитектура мультидоменного гипервизора использовались при разработке распределенной вычислительной системы в ЗАО «РНТ», что подтверждается соответствующими актами об использовании. Разработанная модель безопасности обработки запросов в СиОВ и предложенный принцип мультидоменности для обработчиков запросов использовались при проведении теоретических и практических занятий по дисциплине «Безопасность систем распределенных облачных вычислений» на кафедре «Информационная безопасность компьютерных систем» ФГБОУ ВПО «СПбГПУ» в рамках направлений 090900 «Информационная безопасность» и 090300 «Информационная безопасность вычислительных, автоматизированных и телекоммуникационных систем».

Методология и методы исследования. Для решения поставленных задач использовались системный анализ, теория графов, теория множеств, теория автоматов и методы математического моделирования.

Положения, выносимые на защиту:

1. Формальная модель атаки на средства виртуализации, доказывающая необходимость понижения привилегий эмуляторов устройств в гипервизорах.

2. Оценка степени устойчивости гипервизора к атакам со стороны ВМ, позволяющая сравнить различные реализации гипервизоров.

3. Архитектура мультидоменного гипервизора, обеспечивающая защиту от атак на средства виртуализации.

4. Теорема о монотонности убывания привилегий в ходе обработки запроса пользователя как достаточном условии защищенности от атак на средства виртуализации.

5. Методика обеспечения монотонного убывания привилегий, использующая архитектуру мультидоменного гипервизора.

Степень достоверности научных положений диссертации определяется теоретическим обоснованием предлагаемого аналитического аппарата и результатами их апробации при практическом воплощении.

Апробация результатов работы. Основные теоретические и практические результаты диссертационной работы обсуждались на конференциях:

– VI Международной конференции «MMM-ACNS-2012»;

– XXI научно-технической конференции «Методы и технические средства обеспечения безопасности информации» 24 - 29 июня 2012 г.;

– XIV, XV всероссийской конференции «РусКрипто-2012/2013»;

– Санкт-Петербургской межрегиональной конференции «Информационная безопасность регионов России 2011»;

– XIV Национальном форуме информационной безопасности «ИНФОФОРУМ-2012».

Публикации. По теме диссертации опубликовано 10 научных работ, 4 из которых опубликованы в рецензируемых журналах ВАК РФ.

Объем и структура. Диссертация состоит из введения, четырех глав, заключения и списка источников из 72 наименований.

Основное содержание работы

Во введении обосновывается актуальность темы диссертации, определяется цель, формулируются задачи исследования, описывается структура диссертационной работы.

В первой главе представлены результаты анализа безопасности современных средств виртуализации в системах облачных вычислений, результаты анализа уязвимостей гипервизоров, приведено описание разработанной модели угроз для гипервизоров, которая конкретизирует и дополняет базовую модель угроз ФСТЭК, формулируется задача обеспечения безопасности гипервизора.

Основным недостатком современных гипервизоров является возможность атаки со стороны нарушителя, имеющего доступ к ВМ, на внутреннюю инфраструктуру СиОВ, что подтверждается практическими исследованиями существующих уязвимостей гипервизоров. Для современных гипервизоров базовая модель угроз ФСТЭК является недостаточной. С появлением новых угроз безопасности, обусловленных использованием средств виртуализации, её потребовалось адаптировать и детализировать. В дополнение к базовой модели угроз ФСТЭК в работе предложен новый класс угроз, связанных с преднамеренными или непреднамеренными действиями лиц, имеющих доступ к ВМ (таблица 1). Адекватность предложенной модели подтверждается результатами практических исследований известных уязвимостей (например, CVE-2011-1751 и CVE-2012-0217) средств виртуализации, которые могут служить средством реализации указанных в модели угроз. Защита облачных вычислений от атак на средства виртуализации может быть обеспечена путем минимизации привилегий компонентов гипервизора, уязвимости которых позволяют реализовать подобные атаки. При понижении привилегий уязвимых компонентов гипервизора до минимально допустимых нарушитель не сможет получить преимущества от успешного использования уязвимостей в средствах виртуализации.

Таблица 1 – Угрозы средствам виртуализации в системах облачных вычислений

Угроза	Возможные последствия
Угроза выхода за пределы ВМ	Получение несанкционированного доступа к ресурсам средства виртуализации
Угроза несанкционированного доступа к ресурсам ВМ пользователем другой ВМ	Распространение вредоносного ПО в СиОВ Получение несанкционированного доступа к данным
Угроза несанкционированного доступа к внутренней инфраструктуре СиОВ пользователем ВМ	Получение несанкционированного доступа к данным

Во второй главе описана разработанная формальная модель атаки на средства виртуализации в СиОВ, предложена оценка степени устойчивости гипервизора к атакам, сформулировано условие нейтрализации атак на средства виртуализации и описана архитектура мультидоменного гипервизора.

Анализ известных уязвимостей гипервизоров показал, что класс угроз, связанных с атаками на средства виртуализации, реализуется путем воздействия на эмуляторы устройств, которые создают виртуальную аппаратуру ВМ. При успешной реализации уязвимости хотя бы один эмулятор переходит в состояние, не соответствующее спецификации устройства, в результате чего нарушитель получает возможность влиять на работу гипервизора, используя привилегии уязвимого эмулятора.

Для формулирования условия успешной атаки на гипервизор была разработана формальная модель атак на средства виртуализации. В модели гипервизор представлен как множество конечных автоматов – эмуляторов устройств, а атака на средства виртуализации – это последовательность событий, сгенерированных ВМ. В рамках модели гипервизор H – это множество эмуляторов $\{u\}$, обрабатывающих события из множества $\mathbb{V}$. Множество событий $\mathbb{V}$ состоит из двух непересекающихся подмножеств: V_g – множество событий, генерируемых ВМ, V_h – множество событий,

генерируемых компонентами гипервизора. Эмуляторы устройств располагаются в компонентах $c = (\{u_c\}, Ad_c, Lvl_c)$ гипервизора, обладающих единым адресным пространством Ad_c и уровнем привилегий Lvl_c. Каждый эмулятор описывается конечным автоматом, для которого определен уровень привилегий и функция допустимости состояния: $u = (V_u, S_u, s_0, Tr_u, Sq_u, Lvl_u)$, где $V_u \in \mathbb{V}$ – входной алфавит (множество событий), S_u – множество состояний эмулятора, s_0 – начальное состояние эмулятора при старте ВМ, $Tr_u: S_u \times V_u \to S_u$ – функция перехода между состояниями эмулятора, $Sq_u: S_u \to \{true, false\}$ – функция допустимости состояния, представляющая собой конъюнкцию предикатов, которые характеризуют состояние эмулятора как допустимое или недопустимое, Lvl_u – уровень привилегий эмулятора. В модели рассматривается три уровня привилегий для эмуляторов: У3 соответствует ядру операционной системы, У2 – администратору системы, У1 – непривилегированным компонентам в гипервизоре. Внутренний нарушитель использует для осуществления атаки только события из множества V_g, что подтверждается анализом существующих эксплуатаций уязвимостей гипервизоров. Атака на средства виртуализации представляет собой последовательность из m событий v_i, $i = 1, \dots, m$, которая переводит хотя бы один эмулятор u в гипервизоре H в недопустимое состояние, в результате чего нарушитель повышает свои привилегии в системе до уровня Lvl':

$$Attack = (\{v_i\}_{i=1}^{m}, Lvl', s_t), v_i \in V_g, \exists u \in H: Sq(Tr(s_{t+m}, v_m)) = false, Lvl' = Lvl_u.$$

Из модели следует, что устойчивость гипервизора к атакам на средства виртуализации определяется мощностью множества V_g и уровнем привилегий эмуляторов, обрабатывающих события из этого множества. Для каждого события из множества V_g эмуляторы устройств содержат блоки кода, которые отвечают за его обработку. В работе введено понятие артефакта – блока кода, переводящего хотя бы один эмулятор в другое состояние. Таким образом, каждая атака на средства виртуализации основана на уязвимости в артефакте, но не каждый артефакт содержит уязвимость. Следовательно, множество артефактов в средстве виртуализации сюръективно отображается на множество

уязвимостей в гипервизоре, используя которые нарушитель может совершать атаки на внутреннюю инфраструктуру СиОВ. Количество артефактов β_u в эмуляторе u может быть получено путем анализа исходного кода гипервизора или путем подсчета таких событий из множества V_g, при обработке которых состояние эмулятора изменяется. Поскольку артефакты в эмуляторах, располагающихся в одном компоненте, увеличивают подверженность этого компонента атакам, то оценку степени устойчивости каждого компонента к атакам предлагается вычислять так:

$$\zeta_c = e^{-\varphi}, \varphi = \sum_{u \in \{u_c\}} \beta_u / \sum_{u' \in H} \beta_{u'}.$$

В качестве оценки степени устойчивости гипервизора к атакам предлагается использовать наименьшее среди компонентов с артефактами и самым высоким уровнем привилегий значение ζ_c.

С учетом предложенной оценки степени устойчивости гипервизоров к атакам сформулировано условие нейтрализации атак на средства виртуализации: каждый компонент с $\zeta_c \neq 1$ должен обладать привилегиями, не превышающими минимально необходимые для его работы. Поскольку эмуляторы устройств в компонентах гипервизора требуют различных привилегий, был предложен принцип мультидоменности: эмуляторы должны быть распределены по доменам так, чтобы каждый домен содержал только эмуляторы с одинаковым множеством привилегий. Принцип мультидоменности и принцип наименьших привилегий положены в основу разработанной архитектуры мультидоменного гипервизора (рисунок 1), которая позволяет повысить оценку степени устойчивости гипервизора путем распределения множества эмуляторов по максимальному числу доменов, таким образом, чтобы каждый эмулятор обладал минимально необходимым для его работы множеством привилегий. Предлагаемая архитектура требует, чтобы все эмуляторы находились на уровне привилегий У1. Минимально необходимый набор привилегий эмуляторов определяется ролью гипервизора во внутренней инфраструктуре СиОВ, которая, в свою очередь, обусловлена участием гипервизора в обработке запросов пользователя ВМ.

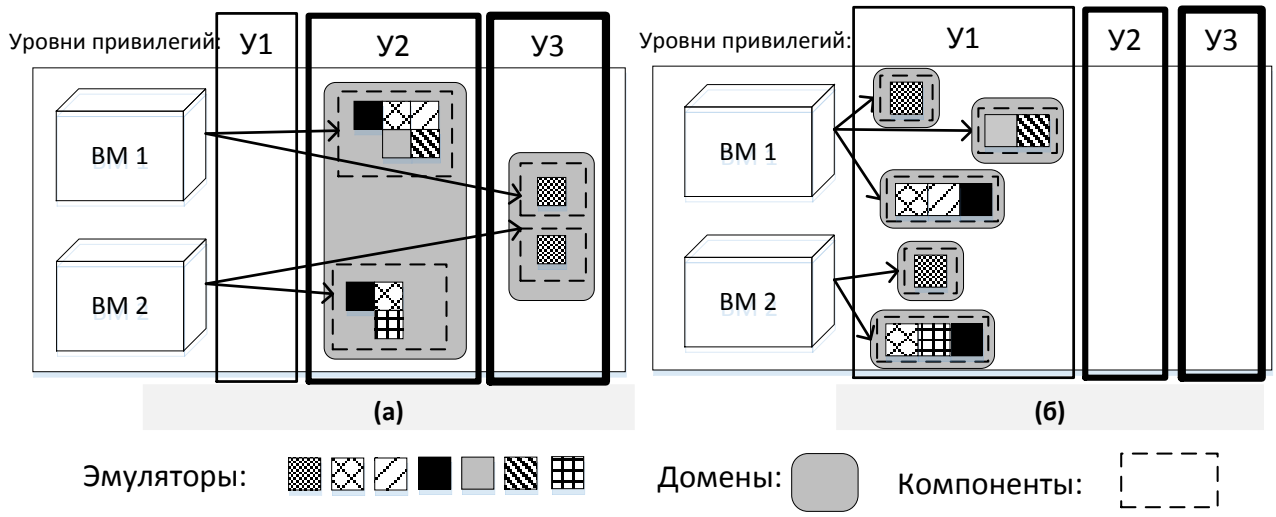

Рисунок 1 – Архитектуры гипервизоров: (а) – традиционного, (б) - мультидоменного

В третьей главе описана разработанная формальная модель безопасной обработки запросов в СиОВ, формализована задача обеспечения безопасности СиОВ и сформулирован принцип наименьших привилегий для обработчиков запросов в СиОВ.

Запросы пользователя СиОВ передаются для обработки сетевым сервисам, приложениям, эмуляторам и другим программам, которые располагаются на различных узлах СиОВ: гипервизоры, ВМ, хранилища, центры управления. В ходе обработки запроса обработчик может сгенерировать новый запрос, направленный другому обработчику, поэтому между запросами в СиОВ существует отношение вложенности, которое описывает их логическую последовательность (рисунок 2).

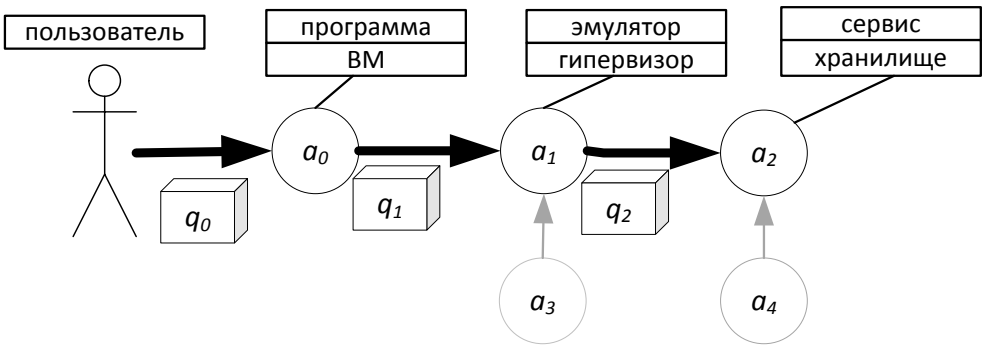

Рисунок 2 – Три последовательных запроса q_0, q_1, q_2 с обработчиками a_0, a_1, a_2, a_3, a_4

В результате анализа работы различных платформ облачных вычислений структура обработки запросов была формализована в виде ориентированного графа, вершинами которого являются обработчики запросов, а дуги соответствуют маршрутам, по которым отправляются запросы другим обработчикам в СиОВ. Разработанная формальная модель обработки запросов в СиОВ представлена в таблице 2. В рамках модели привилегии рассматривались как множество прав доступа, необходимых для выполнения определенных действий.

Таблица 2 – Элементы формальной модели обработки запроса в СиОВ

Множество пользователей системы облачных вычислений	$\mathbb{U}$
Множество вершин графа. Каждая вершина описывается узлом a_{host} и экземпляром программы a_{prog} на нем	$\mathbb{A} = \{(a_{prog}, a_{host})\}$
Множество дуг	$\mathbb{L} = \mathbb{A} \times \mathbb{A}$
Множество привилегий обработчиков запросов	$\mathbb{P}$
Маркировочная функция для вершин графа, ставящая в соответствие обработчику запроса множество его привилегий	$Pl: \mathbb{A} \to \mathcal{P}(\mathbb{P})$ $\mathcal{P}(\mathbb{P})$ – множество подмножеств
Маркированный ориентированный граф обработки запросов в СиОВ	$\mathbb{C} = (\mathbb{A}, \mathbb{L}, Pl)$
Множество всех запросов в СиОВ	$\mathbb{Q}$
Множество запросов, доступных пользователю СиОВ	$Svc: \mathbb{U} \to \mathcal{P}(\mathbb{Q})$
Функция, определяющая для каждого запроса вершину, к которой направлен запрос	$Dest: \mathbb{Q} \to \mathbb{A}$
Функция, для каждого запроса определяющая вершину, которая сгенерировала запрос	$Source: \mathbb{Q} \to \mathbb{A}$
Функция, определяющая для каждого запроса множество вложенных запросов	$Sub: \mathbb{Q} \to \mathcal{P}(\mathbb{Q})$
Функция, сопоставляющая запросу минимально необходимые для его выполнения привилегии	$Pm: \mathbb{Q} \to \mathcal{P}(\mathbb{P})$
Функция, определяющая для заданного множества привилегий множество запросов, которые могут быть отправлены с использованием этих привилегий	$Req: \mathcal{P}(\mathbb{P}) \to \mathcal{P}(\mathbb{Q})$

Для обработки заданного запроса обработчик должен обладать необходимым множеством привилегий, включающим привилегии необходимые для отправки вложенных запросов, если это необходимо. Поэтому для каждой

дуги в графе определено значение функции $Trans$, отображающей множество привилегий вершины a_i в множество эффективных привилегий для связанной вершины a_j, использующихся для обработки запросов из исходной вершины, которые допустимы множеством привилегий P:

$$Trans\colon\ \mathcal{P}(\mathbb{P}) \times \mathbb{L} \to\ \mathcal{P}(\mathbb{P}), Trans\left(P, \left(a_i, a_j\right)\right) = P',$$
$$P' = \bigcup_{q_l \in Req(P)} Pm(q_l) : Source(q_l) = a_i, Dest(q_l) = a_j.$$

Значение функции $Trans$ определяет минимально необходимое множество привилегий для обработки запросов на заданном маршруте. Тогда вычислимо эффективное множество привилегий обработчика, включающее привилегии на вершинах из подграфа:

$$Pt\colon \mathcal{P}(\mathbb{P}) \times \mathbb{A} \to \mathcal{P}(\mathbb{P}), Pt(P, a) = \begin{cases} \emptyset, & P = \emptyset, \\ \widetilde{Pt}(P, a), & P \neq \emptyset, \end{cases}$$

$$\widetilde{Pt}(P, a) = \left(P \cap Pl(a)\right) \cup \left(\bigcup_{a' \in \Gamma^-(a)} Pt(Trans\left(P \cap Pl(a), (a, a')\right), a') \right).$$

ВМ, которые получают запросы непосредственно от пользователя, были названы первичными, поскольку маршруты вложенных запросов от них формируют все остальные подграфы. Для первичной ВМ a минимально необходимое множество привилегий $Ps(a)$ определяется как

$$Ps(a) = \bigcup_{u \in \mathbb{U}} \bigcup_{q \in Svc(u)} \begin{cases} Pm(q), & Dest(q) = a, \\ \emptyset, & Dest(q) \neq a. \end{cases}$$

В работе применялся принцип наименьших привилегий в СиОВ: в ходе обработки запросов привилегии обработчиков не должны превышать привилегии пользователей, инициирующих запросы. В случае соблюдения принципа наименьших привилегий использование уязвимостей в средствах виртуализации не дает нарушителю дополнительных возможностей по доступу к ресурсам облака. Для определения множества минимально необходимых привилегий для обработчиков запросов была доказана теорема:

Теорема 1. Достаточным условием защищенности СиОВ от атак на средства виртуализации является монотонность убывания функции $f(a) = Pt(Pl(a), a)$ по всем маршрутам графа обработки запросов, начинающимся в каждой первичной ВМ a_0, и минимизация привилегий первичных ВМ - $Pl(a_0) = Ps(a_0)$.

Монотонное убывание для привилегий означает, что функция $f(a)$ для любой последовательности вершин, составляющих путь в графе от первичной ВМ a_0 до ВМ a, образует цепь подмножеств, для которых определена частичная упорядоченность на операторе включения. Для обеспечения свойства монотонности убывания необходимо выполнить преобразование графа обработки запросов, не нарушая работы СиОВ.

В четвертой главе приводится разработанная методика обеспечения монотонного убывания привилегий в СиОВ и результаты апробации созданного опытного образца мультидоменного гипервизора.

На основе разработанной модели безопасности обработки запросов предложен алгоритм вычисления множества привилегий доменов, включающих минимально необходимые привилегии для заданного обработчика a: вычислить множество привилегий $T = \{P_i\}$, где $P_i = Trans\big(Pl(a_i), (a_i, a)\big), a_i \in R$, а $R = \Gamma^+(a)$; вычислить не содержащее одинаковых элементов множество $D \subseteq T$ привилегий доменов.

Предложенный алгоритм вычисления множества доменов применим для определения минимально допустимого набора привилегий для эмуляторов в мультидоменном гипервизоре, поскольку учитывает действия, необходимые для обработки событий ВМ, которые требуется совершить компонентам гипервизора в СиОВ.

Для апробации предлагаемого подхода к построению защищенных гипервизоров был создан опытный образец мультидоменного гипервизора (ООМГ) для СиОВ, использующий для контроля привилегий доменов систему безопасности защищенной операционной системы Фебос. Оценки степени устойчивости для ООМГ и других гипервизоров приведены в таблице 3.

Таблица 3 – Значения оценок степени устойчивости гипервизоров к атакам

Гипервизор	Уровни привилегий	Число компонентов на уровне	Максимальное β_c на уровне	Минимальное ζ_c на уровне	Итоговая оценка
Xen	У3	1	194	0,6	0,6
	У2	1	254	0,5	
	У1	0	-	-	
VMware ESXi	У3	1	450	0,3	0,3
	У2	0	-	-	
	У1	0	-	-	
ООМГ	У3	1	0	1	0,8
	У2	0	-	-	
	У1	5	72	0,8	

Для того чтобы система облачных вычислений сохранила работоспособность, к графу обработки запросов должны применяться только следующие преобразования: дублирование вершин и их связей; понижение привилегий вершин до минимально допустимых, определяемых функцией Pm; удаления дуг, которые не являются необходимыми. Указанные преобразования позволяют выполнить декомпозицию обработчиков: вычислить множество $D = \{d_i\}$ привилегий доменов для вершины a; создать $|D|$ дубликатов вершины a и ее связей: $A = \{a_i\}, |D| = |A|$; каждой вершине a_i назначить привилегии d_i домена с номером i; из каждой вершины a_i удалить дуги, для которых $\nexists a_j \in \mathbb{A}: Trans\left(Pl(a_j), (a_j, a_i)\right) = d_i$. Разработанная методика состоит в том, что для обеспечения монотонности убывания привилегий в ходе обработки запросов в системе облачных вычислений необходимо выполнить преобразование графа обработки запросов, соответствующего СиОВ:

1. Построить граф обработки запросов для заданной СиОВ.

2. Вычислить число доменов с минимально необходимыми привилегиями для обработчиков, соответствующих эмуляторам устройств в гипервизорах.

3. Распределить эмуляторы устройств по доменам мультидоменного гипервизора, используя полученное множество доменов.

4. Для каждого обработчика запросов, нарушающего монотонность убывания привилегий в ходе обработки запросов, применить алгоритм декомпозиции обработчика.

Для проверки устойчивости гипервизора к атакам на средства виртуализации была проведена серия практических экспериментов (рисунок 3), имитирующих атаки на средства виртуализации с последующими попытками осуществить несанкционированный доступ (НСД) к ресурсам гипервизора и инфраструктуре СиОВ.

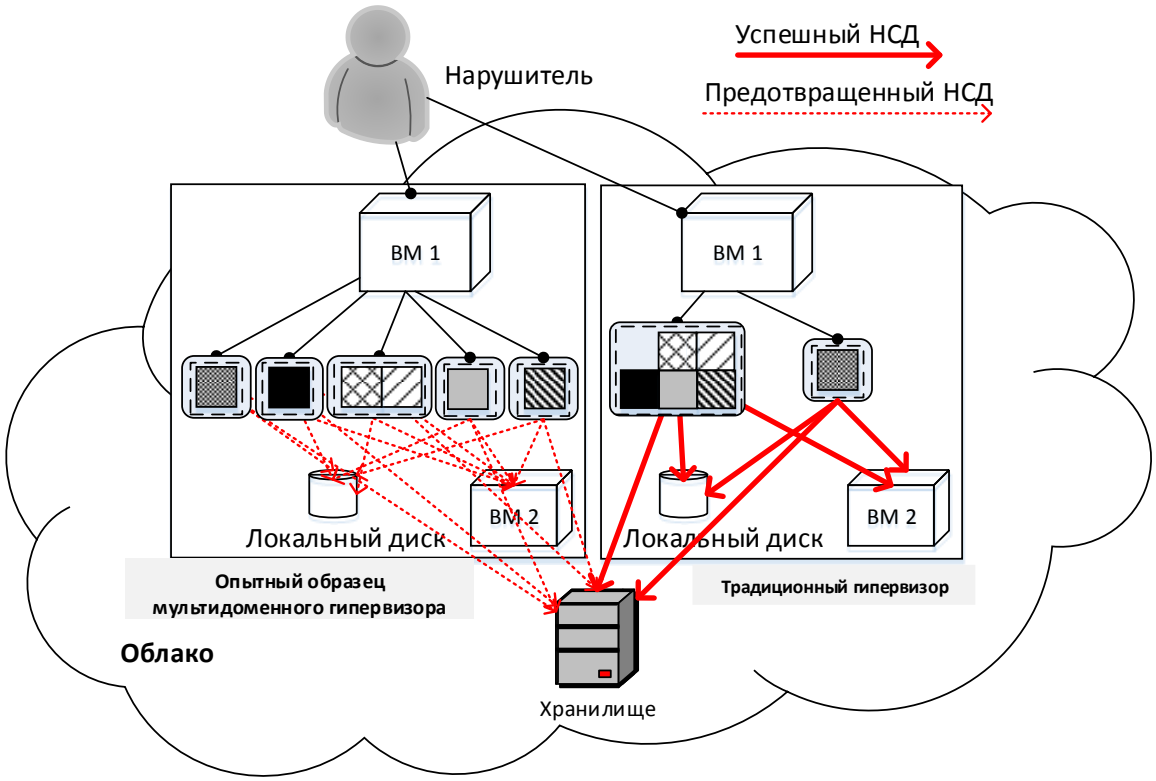

Рисунок 3 – Апробация ООМГ в СиОВ

Для осуществления атаки на гипервизор были сымитированы уязвимости в каждом компоненте разработанного ООМГ и традиционного гипервизора. В результате проведенных экспериментов на обычном гипервизоре действия нарушителя по НСД к ресурсам СиОВ были успешными. На ООМГ все попытки НСД были пресечены, поскольку для совершения НСД требовалось осуществить действия, выходящие за границы доменов.

В заключении приведены результаты и выводы, полученные автором в ходе выполнения работы.

Заключение

В работе получены следующие основные результаты:

1. Построена модель угроз средствам виртуализации в СиОВ, включающая угрозы, связанные с атаками на средства виртуализации.

2. Построена формальная модель атаки на средства виртуализации и предложена оценка степени устойчивости гипервизоров к этим атакам.

3. Разработана архитектура мультидоменного гипервизора, обеспечивающая защиту от атак на средства виртуализации.

4. Разработана формальная модель безопасной обработки запросов в СиОВ и доказана теорема о достаточным условии защищенности СиОВ от класса атак на средства виртуализации.

5. Создана методика обеспечения монотонного убывания привилегий в ходе обработки запросов в СиОВ.

6. Создан опытный образец мультидоменного гипервизора и выполнена его успешная апробация в системе облачных вычислений.

Перспективы дальнейшей разработки темы диссертации заключаются в расширении области применения предложенной мультидоменной архитектуры и разработанной методики для защиты других классов распределенных и вычислительных систем.

Список работ, опубликованных автором по теме диссертации:

1. Никольский, А.В. Формальная модель безопасности гипервизоров виртуальных машин в системах облачных вычислений [Текст] / А.В. Никольский, Д.П. Зегжда // Журнал "Проблемы информационной безопасности. Компьютерные системы". — СПб.: Изд-во Политехн. ун-та, 2013.— № 1. — С. 7–18.

2. Никольский, А.В. Модель угроз гипервизора в системах облачных вычислений [Текст] / А.В. Никольский, Д.П. Зегжда // Журнал "Системы высокой доступности". — Москва: Изд-во Радиотехника, 2013.— № 4. — С. 70–79.

3. Никольский, А.В. Формальная модель для кибер-атак на средства виртуализации и мера уязвимости гипервизоров [Текст] / А.В. Никольский // Журнал "Проблемы информационной безопасности. Компьютерные системы". — СПб.: Изд-во Политехн. ун-та, 2013.— № 3. — С. 40–48.

4. Каретников, А.В. Безопасность облачных вычислений. Проблемы и перспективы [Текст] / А.В. Каретников, Д.П. Зегжда // Журнал "Проблемы информационной безопасности. Компьютерные системы". — СПб.: Изд-во Политехн. ун-та, 2011.— № 4. — С. 7–17.

5. Каретников, А.В. Использование технологии виртуализации при построении защищенных операционных систем [Текст] / А.В. Каретников // Материалы VII Санкт-Петербургской межрегиональной конференции "Информационная безопасность регионов России (ИБРР-2011)" —СПб., 2011. — С.169–170.

6. Каретников, А.В. Безопасность систем облачных вычислений. Проблемы и перспективы [Текст] / П.Д. Зегжда, Д.П. Зегжда, А.В. Каретников // Материалы XIV Национального форума информационной безопасности "ИНФОФОРУМ-2011" — Москва: Изд-во МИФИ, 2011. — С.116–118.

7. Никольский, А.В. Архитектура безопасного гипервизора для построения защищенных систем облачных вычислений [Текст] / А.В. Никольский, Д.П. Зегжда// Сб. материалов 21-й научно-технической конференции "Методы и технические средства обеспечения безопасности информации" — СПб.: Изд-во Политехн. ун-та, 2012. — С. 102–105.

8. Никольский, А.В. Контроль потоков данных во внутри облачных сетях и при взаимодействии кластеров в составе грид-систем [Текст] / А.В. Никольский, Е.А. Таранин, А.Ю. Чернов // Сб. материалов 21-й научно-технической конференции "Методы и технические средства обеспечения безопасности информации" — СПб.: Изд-во Политехн. ун-та, 2012. — С. 114–117.

9. Никольский, А.В. Использование технологии виртуализации для обеспечения защиты платежной информации в системах совершения электронных платежей [Текст] / А.В. Никольский, М.К. Поляков // Сб. материалов 21-й научно-технической конференции "Методы и технические средства обеспечения безопасности информации" — СПб.: Изд-во Политехн. ун-та, 2012. — С. 116–118.

10. Никольский, А.В. Using graph theory for cloud system security modeling [Текст] / П.Д. Зегжда, Д.П. Зегжда, А.В. Никольский // Сб. материалов Шестой Международной конференции "Математические методы, модели и архитектуры для защиты компьютерных сетей" (MMM-ACNS-2012). — Берлин: Изд-во Springer-Verlag Berlin Heidelberg, 2012. — С. 309–318.