На правах рукописи

Борисенко Константин Алексеевич

МЕТОДЫ И МОДЕЛЬ ОРГАНИЗАЦИИ ЗАЩИТЫ ВИРТУАЛИЗИРОВАННЫХ КОМПЬЮТЕРНЫХ СЕТЕЙ РАСПРЕДЕЛЕННЫХ ОБЛАЧНЫХ ВЫЧИСЛИТЕЛЬНЫХ СРЕД ОТ СЕТЕВЫХ АТАК

Специальность: 05.13.15 - Вычислительные машины, комплексы и компьютерные сети, технические науки

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2016

Работа выполнена на кафедре вычислительной техники Санкт- Петербургского государственного электротехнического университета «ЛЭТИ» имени В.И. Ульянова (Ленина).

Научный руководитель: кандидат технических наук,
ведущий научный сотрудник,
Шоров Андрей Владимирович

Официальные оппоненты: доктор технических наук, профессор,
Алиев Тауфик Измайлович,
Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики»,
заведующий кафедрой вычислительной техники

кандидат технических наук, старший научный сотрудник,
Чечулин Андрей Алексеевич
Федеральное государственное бюджетное учреждение науки «Санкт-Петербургский институт информатики и автоматизации Российской академии наук»

Ведущая организация: Публичное акционериное общество "Информационные телекоммуникационные технологии" («Интелтех»), г. Санкт-Петербург

Защита состоится «14» декабря 2016 г. в 17:00 на заседании диссертационного совета Д 212.238.01 Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина) по адресу: 197376, Санкт-Петербург, ул. Проф. Попова, 5.

С диссертацией можно ознакомиться в библиотеке Санкт-Петербургского государственного электротехнического университета «ЛЭТИ» им. В.И. Ульянова (Ленина) по адресу: 197101, Санкт-Петербург, ул. Проф. Попова, д.5 и на сайте: www.eltech.ru

Автореферат разослан «13» октября 2016 г.

Ученый секретарь
диссертационного совета Д 212.238.01
к.т.н., доцент Щеголева Н.Л.

Общая характеристика работы

Актуальность темы диссертации. Технология облачных вычислений является одним из наиболее перспективных направлений развития информационных систем. Преимущественно облачные ресурсы предоставляются по следующим сервисным моделям: Software as a Service (SaaS, программного обеспечение как услуга), Platform as a Service (PaaS, платформа как услуга), Infrastructure as a Service (IaaS, инфраструктура как услуга). Модель IaaS позволяет пользователям создавать виртуализированные компьютерные сети (КС), включающие в себя как виртуальные машины пользователей, так и сервера. Данная технология позволяет клиентам значительно снизить затраты на создание сетевой инфраструктуры, быстро реконфигурировать топологии КС, настраивать виртуальные машины и сервисы. Однако, использование технологий предоставления облачных ресурсов значительно усложняет процесс обеспечения защиты виртуализированных КС. В случае успешного выполнения сетевых атак на виртуализированные КС облачных вычислительных сред (ОВС) или отдельные их узлы, жертвы вредоносного воздействия начинают потреблять большее количество общих ресурсов. Вследствие чего, атака на один конкретный виртуализированный узел КС ОВС может привести к выходу из строя всех элементов КС ОВС, что повышает значимость создания эффективных методов защиты виртуализированных КС ОВС от сетевых атак. Существующие методы защиты не эффективны в условиях высоконагруженных КС ОВС. На текущем этапе развития облачных вычислений выявлен ряд уязвимостей, связанных не только с классическими угрозами для распределенных систем, но и с принципиально новыми, порожденными спецификой виртуализации, а также наличием дополнительных уязвимых компонентов реализующих предоставление облачных услуг. Например, такими компонентами являются компонент администрирования, компоненты организации коммутации сетевого трафика внутри ОВС, компоненты организации предоставления ресурсов для виртуальных машин и др.

На данный момент, большая часть действий по администрированию ОВС, а также защиты ОВС от вредоносных воздействий требует вмешательства системного администратора. Данный способ является неэффективным и трудозатратным. Поэтому возникает необходимость разработки новых моделей, методов и алгоритмов, направленных на выявление проблем функционирования виртуализированных КС ОВС, вызванных вредоносными воздействиями, и их устранением.

Объектом исследования является виртуализированная КС ОВС.

Предмет исследования. Модели и алгоритмы механизмов защиты виртуализированных КС ОВС, основанные на технологии ИАД и методы их моделирования.

Целью диссертационного исследования является разработка методов и модели организации защиты виртуализированных КС ОВС на основе методов интеллектуального анализа данных (ИАД) от сетевых атак.

Для достижения цели были поставлены и решены следующие **задачи**:

1. Анализ современных подходов к организации систем защиты КС ОВС.

2. Разработка методики сбора и анализа трафика, проходящего в виртуализированной КС ОВС.
3. Разработка метода обнаружения и блокировки сетевых атак на виртуализированные КС ОВС, работающего в автоматическом режиме.
4. Разработка метода моделирования сетевых атак и легитимного трафика для экспериментального исследования вредоносных воздействий на виртуализированные КС ОВС и тестирования разработанных методов защиты виртуализированных КС ОВС.
5. Программная реализация компонентов системы защиты виртуализированной КС ОВС, основанной на разработанных моделях и методах.
6. Оценка эффективности разработанной системы.

Методология и методы исследования. В диссертационной работе использовались методы ИАД, в том числе кластерного анализа, машинного обучения, нечеткой логики. Кроме того, для тестирования разработанных компонентов были использованы методы имитационного моделирования, натурного моделирования.

Научная новизна.

1. Разработан метод обнаружения сетевых атак, в отличие от известных, учитывающий динамические изменения структуры и объема легитимного трафика, что позволяет автоматически обнаруживать вредоносные воздействия на виртуализированную КС ОВС с меньшим количеством ошибок первого и второго рода.
2. Предложена модель системы защиты, отличающаяся учетом удаленности вычислительных узлов ОВС друг от друга, в которой реализуется расположение компонентов защиты, что обеспечивает сокращение времени реакции системы защиты на атаки, а также освобождаются ресурсы виртуальных машин (ВМ) ОВС.
3. Разработан метод гибридного моделирования виртуальных сетей и атак, отличающийся от известных интеграцией сети, построенной с использованием метода имитационного моделирования, с виртуализированной, что позволяет за счет получения обучающей выборки выполнить настройку системы защиты.

Практическая значимость исследования. Разработанные модели и алгоритмы могут быть использованы для организации управления сетевыми процессами большинством ОВС, в частности на их основе реализована система для облачной вычислительной платформы OpenStack. Использование разработанных моделей позволит реорганизовать управление ОВС компаниям, предоставляющим решения в сфере облачных услуг, существенно снизив рутинную работу специалистов. Разработанные в процессе исследований стенды для моделирования атак на виртуализированные КС ОВС существенно упрощают процесс тестирования разрабатываемых методов защиты.

Положения, выносимые на защиту.

1. Метод обнаружения сетевых атак, включающий в себя алгоритм переобучения моделей классификации трафика. Разработанный метод учитывает динамическое изменение структуры и объема трафика в виртуализированной КС ОВС. Это позволяет существенно снизить рутинную работу системных администраторов ОВС. Процесс обнаружения сетевых атак состоит из пяти этапов, что позволят снизить ресурсопотребление и количество ошибок первого и второго рода.

2. Метод моделирования внешних и внутренних сетевых атак на виртуализированную КС ОВС. Метод включает в себя модели и алгоритмы гибридного моделирования компьютерных сетей. Методика позволяет комбинировать методы натурного моделирования, имитационного моделирования и эмуляции. Виртуализированные сети воспроизводят процессы, проходящие в реальных компьютерных сетях, с достаточно высокой точностью (поддержка различных сетевых протоколов, последовательности обмена пакетами и т.д.) и минимальными накладными расходами. Реальными узлами выступают ВМ, развернутые в ОВС OpenStack. Подобная комбинация позволяет не только быстро перестраивать топологии компьютерных сетей, настраивать сценарии экспериментов, но и получать более точные результаты по сравнению с имитационным моделированием виртуальных машин и компонентов ОВС.

3. Модель системы защиты для расположения компонент защиты на распределенной ОВС. Использование модели позволит сократить количество компонент защиты при соблюдении параметров. Уменьшение количества узлов защиты позволит системным администраторам тратить меньшее время на обслуживание системы защиты.

4. Архитектура и программный прототип системы мониторинга и реконфигурации виртуальной сети ОВС. Взаимодействие между компонентами выполнено таким образом, чтобы система могла располагаться как на одном узле ОВС, так и быть географически распределенной.

Апробация результатов работы. Основные положения и результаты диссертационной работы докладывались и обсуждались на международных конференциях New2AN, St. Petersburg, Russia, 2016 г.; SEKE’2015, Pittsburgh, USA, 2015 г., ARES’2015, Daejeon, 2015 г. ElConRusW, 2014-2015, Санкт-Петербург, 2014-2015 гг, конференциях профессорско-преподавательского состава СПбГЭТУ «ЛЭТИ», Санкт-Петербург, 2014-2016 гг, международном научном симпозиуме "Sense. Enable. SPITSE.", Санкт-Петербург, 2015 г.

Внедрение результатов работы. Результаты работы были использованы при выполнении НИР и в учебном процессе СПбГЭТУ на кафедре вычислительной техники. Модуль сбора и анализа данных был внедрен корпоративную сеть компании, состоящую из 200 узлов, для выявления проблем, связанных с функционированием сети Интернет.

Обоснованность и достоверность представленных в диссертационной работе научных положений обеспечивается проведением анализа состояния исследований в данной области, подтверждается согласованностью теоретических результатов с практическими, полученными при компьютерной реализации, а также апробацией основных теоретических положений в печатных трудах и докладах на научных конференциях. Достоверность результатов диссертационной работы подтверждается разработкой системы защиты для облачной платформы OpenStack, протестированной в лаборатории безопасности информационных технологии кафедры Вычислительной техники. Кроме того получено экспертное заключение, в котором отмечается достаточность производительности разрабатываемой системы защиты для текущих мощностей сетевых атак, а также отмечается наличие интереса к подобным решениям на мировом рынке.

Публикации. Основные теоретические и практические результаты диссертации опубликованы в 14 научных работах, среди которых 7 работ изданиях, рекомендованных ВАК, 4 работы – в материалах международных научно-технических конференций, 3 свидетельства о регистрации программ для ЭВМ.

Структура и объем диссертационной работы. Диссертационная работа объемом 173 машинописных страниц, содержит введение, четыре главы и заключение, список литературы, содержащий 97 наименований, 9 таблиц, 55 рисунков.

Основное содержание работы

Во введении дано обоснование актуальности темы диссертационного исследования, сформулированы цели и задачи работы, ее научная новизна и практическая значимость, представлены положения, выносимые на защиту.

В первой главе диссертации определена значимость создания новых методов защиты виртуализированных КС ОВС, проведен анализ существующих сетевых атак и механизмов защиты от них, выработаны требования к работе механизмов защиты.

Рассмотрены различные типы ОВС, проведен сравнительный анализ существующих на рынке на текущий момент облачных платформ. Рассмотрены ОВС, предоставляющие услуги: IaaS (Infrastructure as a Service — Инфраструктура в качестве Сервиса), PaaS (Platform as a Service — Платформа в качестве Сервиса), SaaS (Software as a Service — Программное обеспечение в качестве Сервиса).

Проведен анализ сетевых атак на инфраструктуру ОВС. В качестве методов защиты от сетевых атак рассматривалось множество различных подходов, предложена их классификация. Основное внимание уделено механизмам защиты на основе технологии ИАД. Данный подход позволяет создать механизмы защиты, работающие на основе найденных шаблонов потока трафика. Найденные шаблоны являются динамически изменяющимися относительно изменения процессов, происходящих внутри ОВС, например, увеличение или уменьшение количества облачных сервисов. Также определен объект исследования, для которого будет разрабатываться метод защиты.

Сначала опишем модель распределенной ОВС:

$$C = Ac + \sum_{i=1}^{n} V_i ,$$

где C — это все ресурсы ОВС; Ac — контроллер ОВС; V_i — физический вычислительный узел ОВС. В данном случае для упрощения будем считать, что на вычислительном узле установлены необходимые компоненты для коммутации трафика.

Модель виртуализированной КС ОВС:

$$Vnet = \sum_{i=1}^{n} Ln_i, \ \forall Ln_i \in \sum_{i=1}^{m} V_j ,$$

где Ln — это отдельная локальная сеть внутри виртуализированной КС ОВС; n — количество локальных сетей в виртуализированной КС ОВС.

Модель локальной сети состоит из следующих компонентов:

$$Ln_i = \left(\bigcup_{i=1}^{n} VR_i, \bigcup_{j=1}^{m} VM_j, \bigcup_{k=1}^{d} VG_k, \bigcup_{t=1}^{f} VCh_t, \bigcup_{g=1}^{p} R_g \right),$$

при этом $Ln_i \in \bigcup_{a=1}^{b} V_a \mid\Rightarrow d = b,\ b \le n,\ \forall VM_j \in \forall V_a,\ \exists! a \in [1,..,b] : VG_k \in V_a,$

где n — количество всех вычислительных узлов в ОВС; m — количество всех виртуальных машин в КС ОВС; d — количество виртуальных шлюзов выхода в сеть Интернет; f — количество виртуальных каналов связи; p — количество элементов реальной физической сети. В данной модели VR — виртуальный маршрутизатор в КС ОВС; VM — виртуальная машина в КС ОВС; VG — виртуальный шлюз выхода виртуализированной КС в сеть Интернет; VCh — виртуальный канал связи; R — элементы реальной физической сети.

Виртуальные машины одной локальной сети могут использовать ресурсы любой одного из используемых в ОВС вычислительных узлов. Однако, локальная сеть будет распределена по физическим узлам ОВС в зависимости от расположения виртуальных машин. Также один шлюз выхода КС ОВС в сеть Интернет соответствует конкретному вычислительному узлу ОВС. Далее представлены элементы реальной физической сети:

$$R = \sum_{i=0}^{n} RR_i + \sum_{j=0}^{n} RCh_j, \text{где, если } i \neq 0 \mid\Rightarrow j > i,$$

где RR — это физический маршрутизатор, находящийся в сети Интернет; RCh — каналы связи сети Интернет.

Данное диссертационное исследование направлено на разработку методов и модели защиты всех элементов Ln, кроме R.

Рассмотрены различные механизмы мониторинга ОВС. Одним из них является перенаправление трафика через узел мониторинга, определяющего источники, формирующий вредоносный трафик. Основной идеей данного подхода является недоступность защищаемого сервера в сети Интернет. Весь трафик до него идет через узел мониторинга, который верифицирует клиентов и отвечает на запросы. Данный подход к защите от неавторизированных попыток доступа к внутренней инфраструктуре не видит разницу между вредоносными пакетами и не может управлять межсетевым экраном для фильтрации нежелательного трафика. Следующий вариант защиты от вредоносных воздействий заключается в перенаправлении каждого нового соединения между клиентом и защищаемым сервером через сторонний сервер, который каждый раз создает новый маршрут до сервера. Данный подход эффективен лишь от воздействий, направленных на ограничение пропускной способности канала, однако не подойдет для защиты узлов, находящихся непосредственно перед ОВС, как и от других вредоносных воздействий. Широкое распространение получили системы, использующие сигнатурный поиск аномалий в трафике. В основном подобные системы защиты анализируют поведение злоумышленника линейно, сравнивая поток трафика с образцами потоков, создающимися атаками smurf, SYN Flooding или другими известными типами атак. Подобные решения эффективны против злоумышленников, использующих широко распространенное программное обеспечение и стандартные сценарии проведения атак, но

не справятся с необычными способами, которые злоумышленник может предпринять. Кроме того, в случае, обнаружения источника вредоносного трафика, система заблокирует его полностью, хотя это может быть легитимный клиент, зараженный вирусом. В случае с ОВС, блокировка целиком внутренней виртуальной машины может повлечь большие проблемы для клиента, а в последствие, и для провайдера облачных сервисов, так как основной целью использования ОВС является доступность ресурсов и сервисов 24/7/365.

Исходя из вышесказанного, поставлена следующая задача диссертационного исследования: разработка моделей, методик и алгоритмов, позволяющих производить автоматический мониторинг состояния ОВС, а также создание программных средств, основанных на разработанных методах.

Во второй главе представлены метод и модель обеспечения защиты виртуализированной КС ОВС, описаны требования к системе защиты КС ОВС, метод моделирования вредоносного и легитимного трафика. Метод обнаружения и блокировки вредоносного трафика в виртуализированной КС ОВС представляет собой действия оператора и системы защиты. Метод состоит из трех этапов: подготовительного, первичного обучения моделей классификации трафика и определения параметров сетевых атак. В основе обнаружения трафика лежат модели классификации с учителем. Метод содержит алгоритм переобучения моделей, адаптирующий систему защиты относительно изменений структуры и объема трафика в КС ОВС (рис. 1).

Метод разделен на три основных этапа: (1) подготовительный этап, (2) первичное обучение системы защиты, (3) запуск системы защиты.

Процесс обнаружения параметров вредоносного трафика состоит из двух уровней: на первом уровне определяется наличие вредоносной активность в КС ОВС, второй уровень состоит из четырех этапов: первый этап определяет жертв вредоносной активности, второй — источники, создающие вредоносный трафик, третий — тип трафика портов источников, четвертый — классификация типа трафика связок IP-адресов и портов источника с узлом назначения. После обнаружения параметров вредоносного трафика запускается алгоритм выбора способа блокировки трафика.

В случае если трафик был классифицирован как легитимный, то в случае степени уверенности, больше заданной оператором, в принадлежности трафика к легитимному, данные о нем передаются для адаптации моделей ИАД. Так как структура виртуализированной КС ОВС динамична — постоянно добавляются новые клиенты и сервисы, то в какой-то момент может оказаться так, что система защиты начнет классифицировать трафик с большим количеством ошибок первого рода, а именно, когда легитимный трафик будет классифицирован как вредоносный.

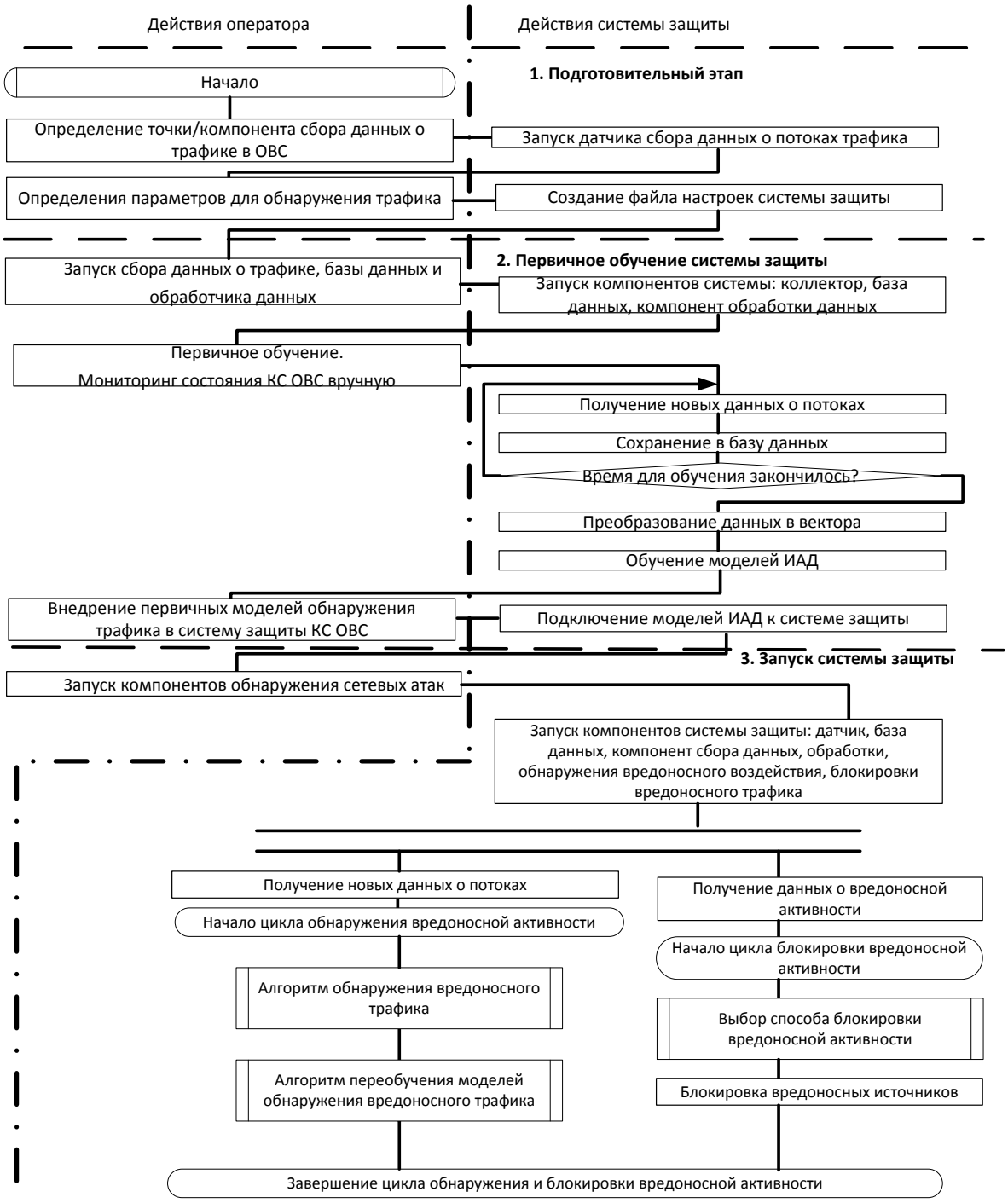

Рисунок 1 — Обобщенный метод обнаружения и блокировки сетевых атак

Чтобы избежать подобных ошибок был разработан алгоритм адаптации моделей ИАД (рис. 2). В результате данные о трафике отправляются в базу данных для дальнейшего переобучения моделей. В соответствии с заданными оператором настройками раз в заданное время модели переобучаются.

Описанный выше метод организует защиту одного вычислительного узла ОВС. Далее будет рассмотрены требования к расположению компонент системы защиты для распределенной ОВС.

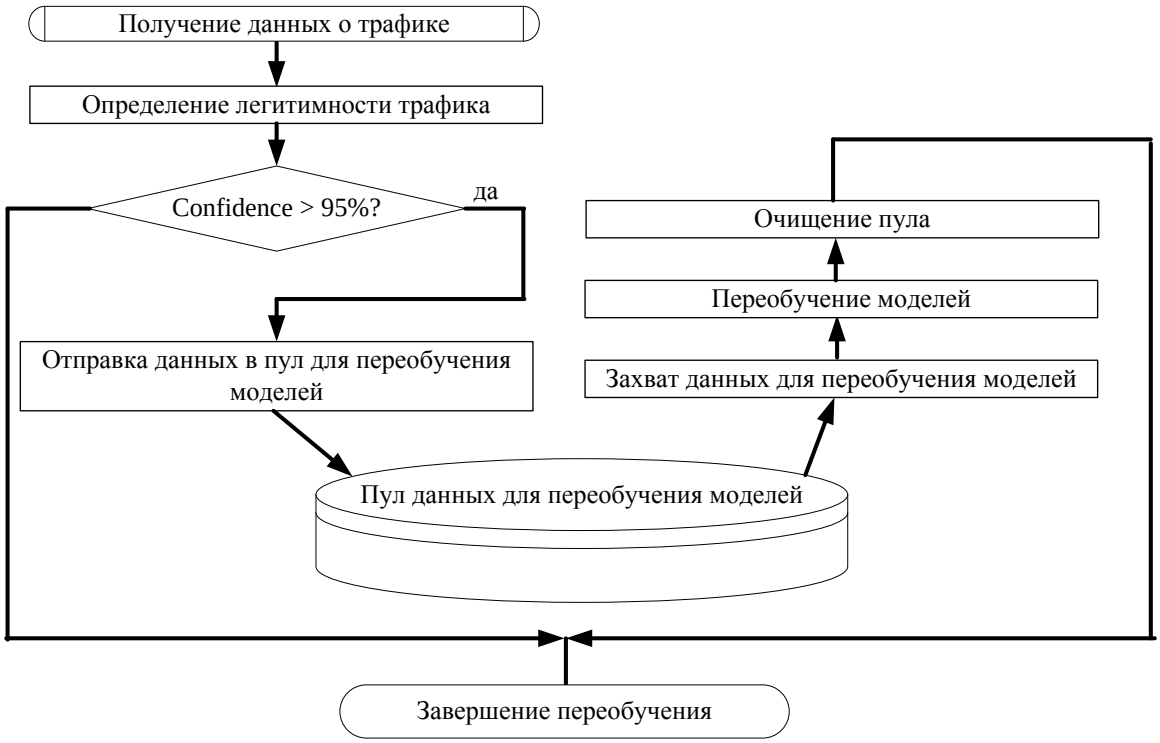

Рисунок 2 — Алгоритм переобучения моделей ИАД для адаптации к изменениям в структуре трафика в КС ОВС

Рассмотрим модель отдельного вычислительного узла с параметрами удаленности от других вычислительных узлов:

$$V_i = VG_i + Vnet_i + \bigcup_{\substack{j=1 \\ j \neq i}}^{n} t_{ij} + AvgSpeed_i,\ i, j \in [1..n],$$

где n — количество вычислительных узлов, V — вычислительный узел; VG — виртуальный шлюз выхода КС ОВС в сеть Интернет; Vnet —часть виртуализированной КС ОВС, которая использует ресурсы данного вычислительного узла; $t_{i,j}$ — длительность отправки сообщения от i-го вычислительного узла до j-го; AvgSpeed — средняя скорость легитимного потока трафика в КС ОВС.

Расстояние между вычислительными узлами можно представить в виде нижней унитреугольной матрицы:

	V_1	V_2	V_3	...	V_n
V_1	1	0	0	...	0
V_2	t_{21}	1	0	...	0
V_3	t_{31}	t_{32}	1	...	0
...	...	...	...	...	...
V_n	t_{n1}	t_{n2}	t_{n3}	...	1

Главной диагональной данной матрицы является расстояние каждого вычислительного узла до себя самого. Это значение не превышает одной миллисекунды.

От дальности расположения вычислительных узлов друг от друга и от системы защиты напрямую зависит длительность задержки обработки потоков трафика, обнаружения атак и их блокировки. Также в зависимости от мощности трафика, проходящего в КС ОВС зависит время его обработки. Кроме того, скорость обработки трафика и работы системы защиты в целом зависит от ресурсов, зарезервированных для системы защиты, основным из которых является процессорная мощность. Рекомендации по мощности трафика, обрабатываемого системой защиты далее будут даны относительно использованного в проведенных тестах ПК:

1. ЦПУ: Inter Core 2 duo, 2,8 ГГц;
2. ОЗУ: 4 Гб, 1333 Mhz.

Рассмотрим модель системы защиты:

$$S = \left\{ D_{вх}, f\left(D_{вх}\right), A_{f\left(D_{вх}\right)}, B_A, D_{вых}, V_{осн} + \bigcup_{j=0}^{n} V_j \right\},$$

$$\text{где } n = k, \text{ если} \begin{cases} \forall t_{осн,g} \le 200\,\text{ms} \text{ для } g \in [0,..,k] \\ \sum_{i=0}^{n} \text{AvgSpeed}_i \le 350\ \text{Mbit/s} \text{ для } i \in [0,..,k] \end{cases}$$

$D_{вх}$ — это множество данных о потоках трафика:

$$D_{вх} = \bigcup_{i=1}^{n} A_i = \sum_{j=1}^{m} \bigcup_{l=0}^{k} A_{l,j},$$

где m — это количество вычислительных узлов, обслуживаемых системой защиты; j — номера обслуживаемых вычислительных узлов; A_i — это множество данных о потоке трафика, а n — количество потоков, собранных для анализа.

$f\left(D_{вх}\right)$— это функция преобразования $D_{вх}$ в векторы для моделей классификации трафика:

$f\left(D_{вх}\right) = \left[\mu_{i,j}\right]$, где i = 1..N, где N — количество различных вариантов, принадлежащих фильтру ($N \le n$), j = 1..3 — соответствующий номер атрибута вектора

$\mu_{i,1} = \sum_{k=1}^{N_i} d_{\text{байт}_k}$; $\mu_{i,2} = \sum_{k=1}^{N_i} d_{\text{пакетов}_k}$, где $d_{байт}$ и $d_{пакетов}$ — количество байт и пакетов в потоке.

Пусть U_i=[(Srcip:port_Dstip:port)$_k$] является множеством всех связок IP-адресов и портов в i-ом фильтре. Тогда U'_i=[(Srcip:port_Dstip:port)$_k$] множество таких связок, что для $\forall k : k \ne l \Rightarrow (Srcip : port\_Dstip : port)_k \ne (Srcip : port\_Dstip : port)_l$

$$U' = \bigcup_{i=1}^{N'_i} U'_i,\ \mu_{i,3} = N'_i$$

$A_{f\left(D_{вх}\right)}$ — алгоритм обнаружения вредоносных источников. B_A — алгоритм выбора способа блокировки вредоносных источников. $D_{вых}$ — данные для межсетевого экрана и о заблокированных источниках, $t_{осн,g}$ — это длительность обмена пакетом между «основным», выбранным в качестве начального вычислительного узла для обеспечения защиты, и другим физическим вычислительным узлом распределенной ОВС.

Для анализа трафика используется модели классификации ИАД, поэтому необходимо создать обучающую выборку для легитимного и вредоносного трафика. Для получения данных о вредоносном и легитимном трафике был разработан метод моделирования трафика с использованием методов гибридного моделирования, включающего натурное и имитационное моделирование (рис. 3).

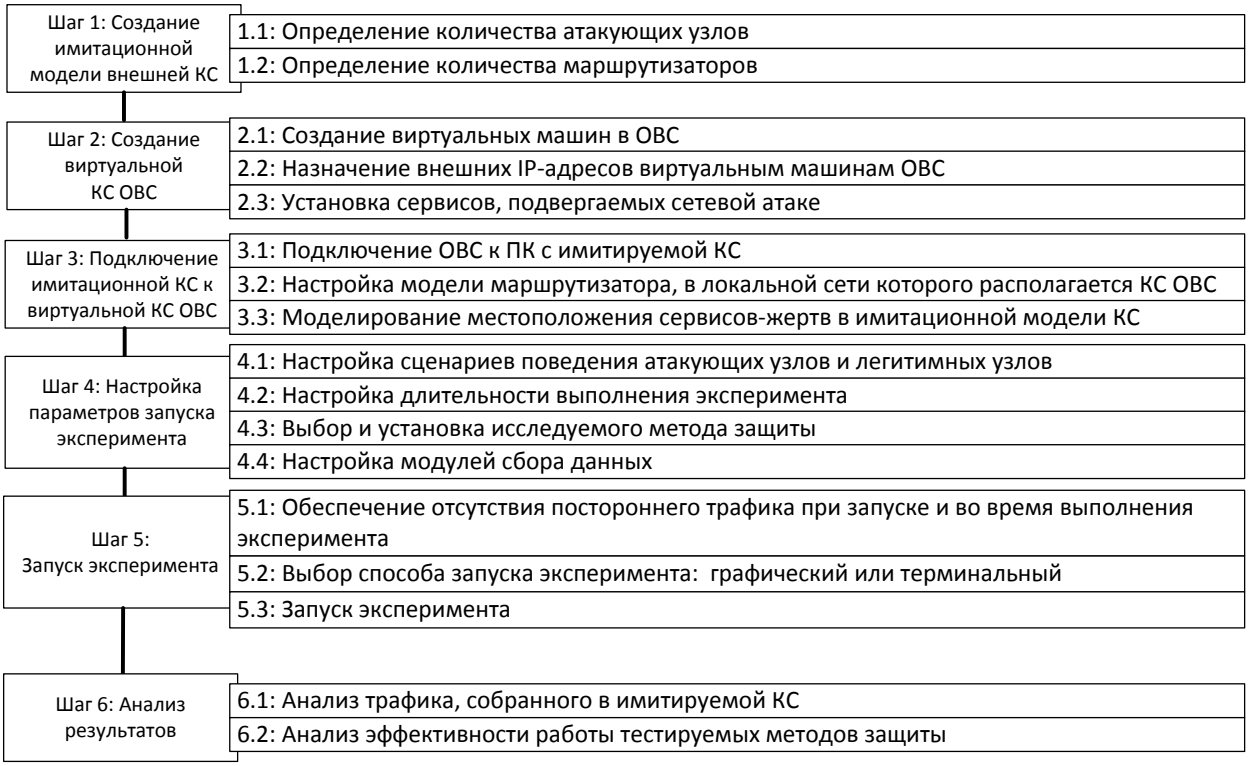

Рисунок 3 — Метод моделирования внешних и внутренних сетевых атак на виртуализированную КС ОВС

В соответствии со спецификой моделирования процессов защиты в ОВС предложено объединение использования имитационного моделирования для создания многоуровневых компьютерных сетей с натурным моделированием, а именно подключением реальной облачной платформы к имитационной сети. Такой подход позволит избежать временных и финансовых затрат на покупку и создание компьютерных сетей и на их настройку создания и оценки эффективности методов и моделей защиты КС ОВС. Кроме того, подключение реальной облачной платформы позволит увеличить точность проведения экспериментов и также сократить время на имитацию компонентов облачной платформы. Разработанный полигон был успешно верифицирован на соответствие необходимым для моделирования трафика характеристикам реальных сетей, построенных в проекте PlanetLab.

Третья глава посвящена архитектуре системы защиты (рис. 4) и ее реализации для ОВС. Также в главе была проанализирована архитектура и взаимодействие между компонентами ОВС OpenStack.

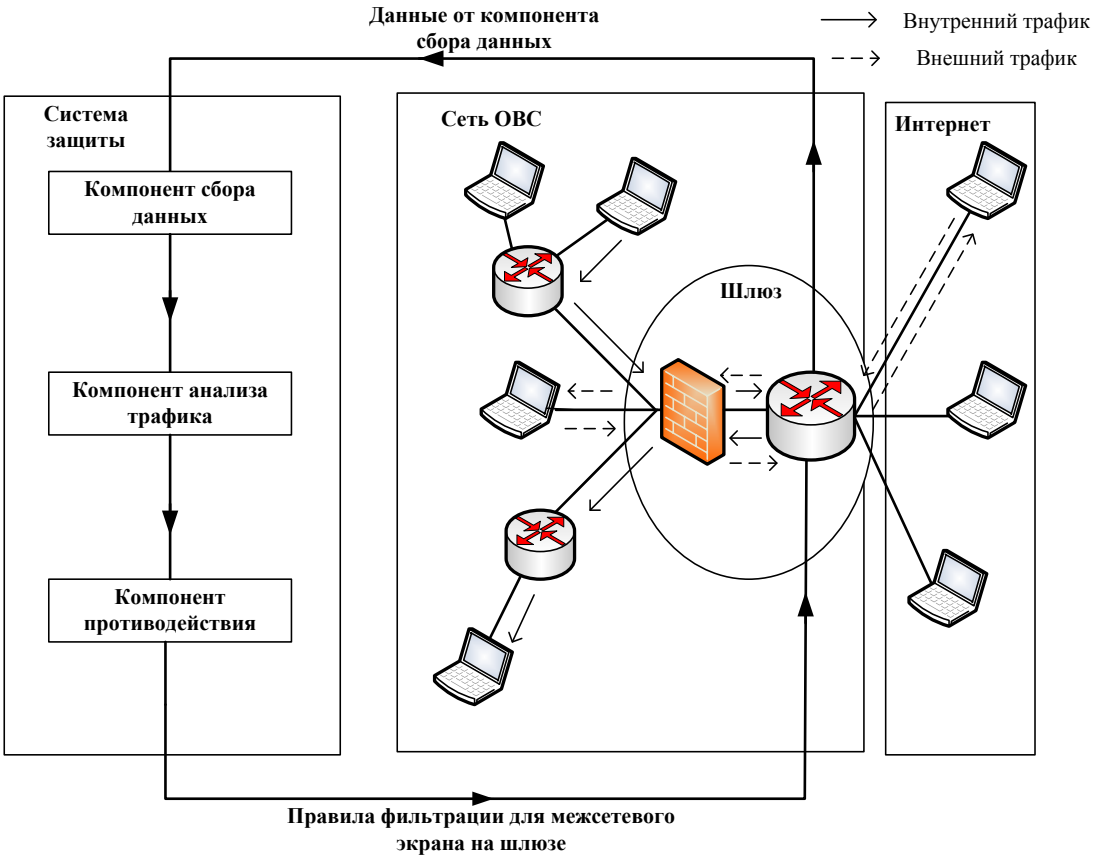

Рисунок 4 — Архитектура системы защиты виртуализированных КС ОВС от сетевых атак

Предлагаемая архитектура системы защиты виртуализированных КС ОВС иерархическая и включает в себя следующие компоненты: датчик, собирающий информацию о трафике; коллектор, хранящий информацию о трафике и преобразующий ее к виду, необходимому компонентам принятия решений; компонент определения источников и жертв вредоносного трафика включает в себя два уровня: первый уровень определяет наличие или отсутствие вредоносного трафика в виртуализированных КС ОВС, второй уровень активируется в случае наличия вредоносного трафика и передает информацию об источниках атак на компонент противодействия атакам; компонент противодействия атакам выбирает оптимальный вариант отражения атаки на основании информации, полученной от предшествующих компонент. В главе рассмотрены методики сбора трафика. Для сбора данных о трафике был выбран Netflow-протокол, собирающий информацию о потоках трафика, не затрагивая содержимого пакетов. Описаны компоненты сбора данных, хранения данных, анализа трафика и противодействия сетевым атакам, также представлено их взаимодействие друг с другом.

В четвертой главе производится экспериментальная оценка эффективности описанных формальных моделей. Представлен сравнительный анализ эффективности работы различных моделей ИАД.

Проведена оценка эффективности работы моделей обнаружения наличия внутренних и внешних атак на ОВС, поиска источника атак.

Была проведена серия экспериментов с различными сценариями внутренних атак для оценки моделей ИАД. В качестве легитимного трафика создавался Netflow-трафик,

идентичный реальному. В случае HTTP Flooding была достигнута максимально возможная мощность на развернутом стенде — 1 Гбит/с.

Анализ эффективности работы компонента хранения данных о потоках трафика представлен на (рис. 5, 6).

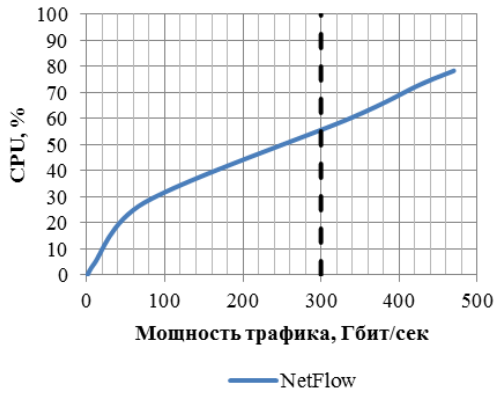

Рисунок 5 — Зависимость загрузки CPU модулем сбора и обработки данных от мощности создаваемого трафика

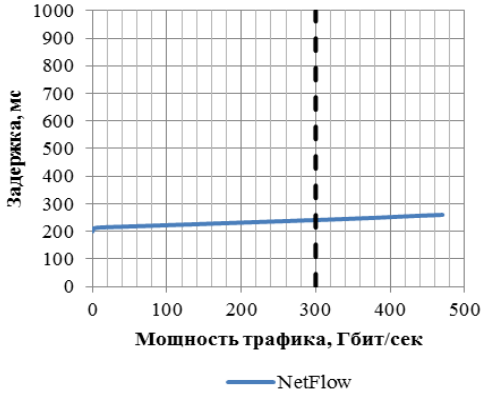

Рисунок 6 — Зависимость задержки сохранения данных от мощности создаваемого трафика

Была оценена эффективность работы моделей ИАД для каждого из этапов. В результате в ходе экспериментов было получено 5 моделей ИАД для двух уровней мониторинга виртуализированных КС ОВС. Процент ошибок первого рода всех моделей не превышает 6%. Чем меньше данный процент, тем меньшее количество пользовательского трафика будет помечено вредоносным и будет пропущено в облачную сеть. Для снижения данного значения была выдвинута гипотеза: обезличивание типа вредоносного сценария снизить процент ошибок первого рода. В случае если запись в базе данных соответствует SYN Flooding или HTTP Flooding, то ее тип был переименован в Malicious. На преобразованных данных были обучены те же самые модели. Результаты представлены в таблице 1.

Таблица 1. Сравнение результатов работы моделей без объединения вредоносных типов атак и с объединением

		1 уровень	**2 уровень**			
			1 этап	**2 этап**	**3 этап**	**4 этап**
Syn, Http, Benign	**FPR, %**	0	3.78	3.77	5.45	4.95
	FNR, %	0.03	0.87	0.86	0.01	0.007
Malicious, Benign	**FPR, %**	2.04	*1.11*	3.99	*4.49*	*3.98*
	FNR, %	0	*0.54*	0.802	*0.01*	*0.007*

Главным критерием определения наиболее эффективной модели будем считать минимальный процент ошибок первого рода (FPR, FPR=FP/(FP+TN)). Для первого уровня гипотеза обезличивания типа вредоносного трафика не оправдалась. Для второго уровня гипотеза оправдалась для первого, второго и третьего этапов. При это процент ошибок первого рода в случае объединения вредоносных типов трафика уменьшился на 25% по сравнению с результатом, полученным без объединения типов. Гипотеза оправдала себя на трех моделях из пяти.

В результате для компонента обнаружения вредоносных источников для 1 уровня будет использоваться модель без объединения типов вредоносного трафика, для 2 уровня: 1, 3, 4 этапы — модели с объединением типов вредоносного трафика, 2 этап — без объединения.

Рассмотрим результат работы системы защиты целиком, а не каждого этапа по отдельности. На первом уровне легитимный трафик определяется со 100 точностью и не может быть триггером для активации второго уровня. В случае активации второго уровня на первом этапе неверно определяется 1,11% всего легитимного трафика. То есть 1,11% легитимного трафика будет классифицироваться на следующем этапе. На 2 этапе 3,77% трафика определяется неверно. То есть на следующий этап перейдет всего лишь 0,04% легитимного трафика. В результате работы 3 этапа на последний этап перейдет 0,0018% легитимного трафика. В результаты работы компонента обнаружения вредоносного трафика процент неверно классифицированного трафика составит около $7{,}5*10^{-5}$%. В отсутствие вредоносного трафика весь легитимный трафик определяется верно, во время сетевой атаки при мощности легитимного трафика в 100 Мбит/с лишь 78 бит/с трафика может быть определено как вредоносный. Результаты тестирования разработанной системы защиты превышают результаты работы существующих решений, описанных в предыдущих разделах (основываясь на обзорах данных решений). Однако, в случае если внешний источник генерирует и вредоносный трафик, и легитимный, то он будет полностью недоступен и легитимный трафик будет также заблокирован.

Основываясь на результатах экспериментов при мощности вредоносного трафика 400 Гбит/с система защиты не заблокирует лишь 2,9 Кбит/с ($6*10^{-7}$%), что является очень высоким показателем надежности работы системы защиты.

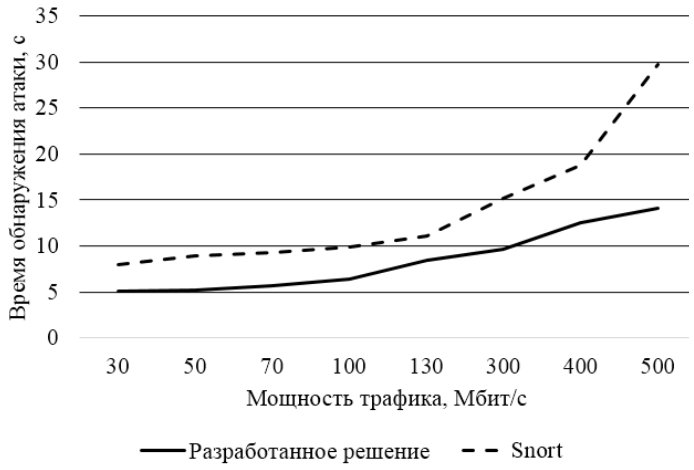

Рисунок 7 — Сравнение времени обнаружения вредоносной активности при комбинированном сценарии атаки

Далее было выполнено сравнение эффективности разработанного решения по защите виртуализированных КС ОВС с программой Snort. Рассмотрим результаты эксперимента с комбинированными сценариями атак (рис. 7).

В данном случае увеличение времени обнаружения больше зависит для разработанного решения, однако, Snort менее эффективен. Следует отметить, что результаты Snort'а являются временем получения первого предупреждения о вредоносном трафике. Это предупреждение отражает IP-адрес и порт, с которого идет вредоносный трафик. Для разработанного решения результатом является выдача полной информации о всем состоянии сети: список вредоносных IP-адресов и портов.

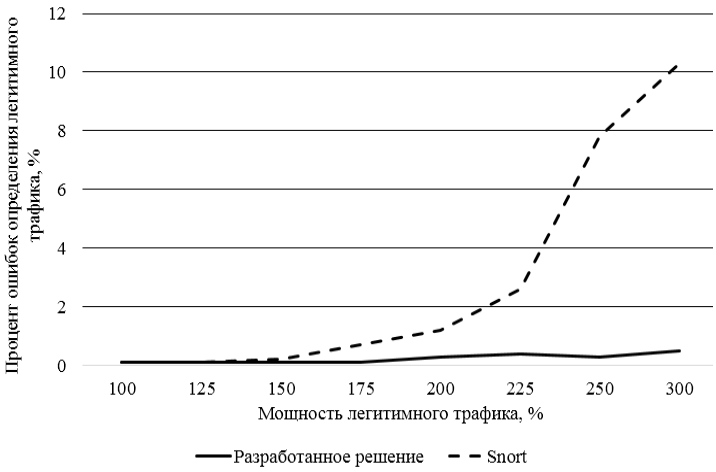

Рисунок 8 — Сравнение количества ошибок при увеличении мощности легитимного трафика

Далее приведены результаты экспериментов с моделированием динамического увеличения количества виртуализированных узлов и легитимного трафика в КС ОВС. В течение четырех часов мощность легитимного трафика увеличивалась постепенно со 100% до 300%. Для Snort были добавлены вручную правила обнаружения вредоносного трафика, основывающиеся на количестве пакетов за период времени. Правила, изучающие payload пакетов, были отключены. Результаты представлены на рисунке 8.

При несущественном увеличении мощности легитимного трафика Snort не уступает в верном определении легитимного трафика, однако при увеличение мощности более чем в два раза, количество ошибок начинает стремительно расти. Благодаря адаптации к изменениям трафика, разработанная система обнаружения вредоносного трафика с увеличением мощности изменяет модели ИАД, что позволяет верно классифицировать трафик. В результате при трехкратном увеличении легитимного трафика процент неверной классификации у разработанного решения не превышает 0,5%.

Изучая результаты научной деятельности последних лет в данном направлении, стоит отметить узкую специализацию моделей и методов, разрабатываемых исследователям. Данные модели и методы полностью не решают проблему обеспечения защиты от сетевых атак на виртуализированные КС ОВС, при этом в большинстве случаев задействуется клиентская часть и отсутствует возможность блокирования отдельных портов, генерирующих вредоносный трафик.

В заключении сформулированы основные результаты работы:

1. Был проведен анализ современных подходов к организации систем защиты в ОВС. На основе рассмотренных работ был выбран подход, использующий ИАД для классификации сетевого трафика.
2. Были разработаны методики сбора и анализа трафика, проходящего в КС ОВС. В основе сбора данных лежит Netflow-протокол, позволяющий сформировать необходимые векторы данных для моделей классификации. Тестирование показало, что быстродействие и ресурсопотребление данных компонентов соответствует текущим требованиям к обработке вредоносного трафика.
3. Разработан метод обнаружения сетевых атак на КС ОВС, работающий в автоматическом режиме. Определена модель расположения компонентов системы защиты для распределенной ОВС. Представленная модель позволяет уменьшить количество элементов системы защиты, тем самым снижая необходимую ресурсную мощность для функционирования системы защиты.

Разработанный процесс выявления проблем функционирования сетевой инфраструктуры ОВС состоит из пяти этапов, что позволяет во время отсутствия вредоносного трафика снизить ресурсопотребление системой защиты, а при наличии вредоносного трафика повысить точность обнаружения и блокировки сетевых атак.

4. Для создания обучающей выборки и тестирования разработанных моделей, методов и алгоритмов был разработан метод гибридного моделирования сетевых атак и легитимного трафика. Метод отличается более быстрым созданием многоуровневых сетей и более точным выполнением экспериментов относительно методов натурного и имитационного моделирования. Разработанный на основе предложенного метода полигон был успешно верифицирован на соответствие реальным сетям, построенным в проекте PlanetLab.
5. На основе разработанных методов, моделей и алгоритмов была выполнена программная реализация компонентов системы защиты виртуализированных КС ОВС от сетевых атак.
6. Реализованная система защиты была протестирована, используя разработанный полигон. Основными метриками оценки результатов были выбраны количество ошибок первого и второго рода, а также время обнаружения вредоносного трафика. Было выполнено сравнение эффективности работы системы защиты КС ОВС с существующим решением по обнаружению вредоносного трафика Snort. В результате множества экспериментов был сделан вывод о более эффективной работе предлагаемого решения.

Публикации в журналах, входящих в перечень ВАК

1. Борисенко, К. А. Моделирование DDoS-атак и механизмов защиты от них / Я. А. Бекенева, Н. Н. Шипилов, К. А. Борисенко, А. В. Шоров // ИЗВЕСТИЯ СПбГЭТУ «ЛЭТИ». – 2015. – №3. – С. 32-40.

2. Борисенко, К. А. Система имитационного моделирования для разработки и тестирования методов защиты от DDoS-атак с возможностью подключения реальных узлов / К. А. Борисенко, Я. А. Бекенева, Н. Н. Шипилов, А. В. Шоров. // ИЗВЕСТИЯ СПбГЭТУ «ЛЭТИ». – 2015. – № 6. – С. 22-29.

3. Борисенко, К.А. Модуль обработки сетевых данных для обнаружения инфраструктурных атак в облачной вычислительной среде OpenStack / А. В. Смирнов, К.А. Борисенко, Е.С. Новикова, А. В. Шоров, И. В. Петухов // ИЗВЕСТИЯ СПбГЭТУ «ЛЭТИ». – 2016. – №4. – С. 24-30.

4. Borisenko, K. Detecting the Origin of DDoS Attacks in OpenStack Cloud Platform Using Data Mining Techniques / K. Borisenko, A. Rukavitsyn, A. Gurtov, A. Shorov // Internet of Things, Smart Spaces, and Next generation Networks and Systems. – 2016. – P. 303-315.

5. Borisenko, K. Investigation of DDoS Attacks by Hybrid Simulation / Ya. Bekeneva, K. Borisenko, A. Shorov, I. Kotenko // Information and Communication Technology. Springer International Publishing. – 2015. – P. 179-189.

6. Борисенко, К. А. Система имитационного моделирования для разработки и тестирования методов защиты от ddos-атак с возможностью подключения реальных узлов/ К.А. Борисенко, Я.А. Бекенева, Н.Н. Шипилов, А.В. Шоров // Безопасность информационных технологий. – 2015. – №4. – С. 6-17.

7. Borisenko, K. Framework for Infrastructure Attack Modeling in Hybrid Networks / K. Borisenko, I. Kholod, A. Shorov // International Journal of Mobile Computing and Multimedia Communications. – 2014. – №6(4). – P. 98-114.

Другие статьи и материалы конференций

8. Borisenko, K. Distributed Execution Environment for Data Mining as Service / I. Kholod, K. Borisenko // Proceedings of the 2016 IEEE North West Russia Section Young Researches in Electrical and Electronic Engineering Conference. Saint Petersburg, 2-3 Febr. 2016 y. – Saint Petersburg, 2016. – P. 244-249.

9. Borisenko, K. DDoS Attacks in Cloud Computing Using Data Mining Techniques / K. Borisenko, A. Smirnov, E. Novikova, A. Shorov // 16th Industrial Conference, ICDM 2016, New York, NY, USA, July 13-17, 2016. Proceedings. – Springer, 2016. – P. 197-211.

10. Borisenko, K. Simulation of DDoS-attacks and Protection Mechanisms against Them / Ya. Bekeneva, N. Shipilov, K. Borisenko, A. Shorov // Proceeding of 2015 IEEE North West Russia Section Young Researchers in Electrical and Electronic Engineering Conference (2015 ElConRusW). Saint Petersburg, 2-4 Febr. 2015 y. – Saint Petersburg, 2015. – P. 50-56.

11. Borisenko, K. Modeling Framework for Developing and Testing Network Security Techniques against DDoS Attacks / K. Borisenko, I. Kholod, A. Shorov // Proceedings of the 27th International Conference on Software Engineering and Knowledge Engineering (SEKE 2015). – Pittsburgh, 6-8 July 2015. – Skokie.: KSI Research Inc., 2015. – P. 715.

Свидетельства о государственной регистрации программы для ЭВМ

12. Борисенко, К.А. Система обучения пошаговой реализации алгоритмов с помощью конечного автомата: Свидетельство о государственной регистрации программы для ЭВМ №2015614670 / К.А. Борисенко, А.М. Чамкин; правообладатель ФГБОУ СПбГЭТУ «ЛЭТИ». – Зарегистрировано в Реестре программ для ЭВМ 23 апреля 2015 г.

13. Борисенко, К.А. Программа для имитационного моделирования DDoS-атак и разработки методов защиты от них с возможностью подключения реальных узлов: Свидетельство о государственной регистрации программы для ЭВМ №2015618808 / К.А. Борисенко, Н.Н. Шипилов, А.В. Шоров; правообладатель ФГБОУ СПбГЭТУ «ЛЭТИ». – Зарегистрировано в Реестре программ для ЭВМ 19 августа 2015 г.

14. Борисенко, К.А. Программа сбора данных для получения количественных характеристик трафика в высоконагруженных компьютерных сетях: Свидетельство о государственной регистрации программы для ЭВМ №2016614418 / К.А. Борисенко, А.Н. Рукавицын, А.В. Шоров; правообладатель ФГБОУ СПбГЭТУ «ЛЭТИ». – Зарегистрировано в Реестре программ для ЭВМ 22 апреля 2016 г.