УДК 004.056

Волокита А.Н., Сайко В.Г., Ву Дык Тхинь

СПЕЦИАЛИЗИРОВАННЫЕ АГЕНТЫ БЕЗОПАСНОСТИ ДЛЯ ЛОКАЛИЗАЦИИ ВТОРЖЕНИЙ В РАСПРЕДЕЛЕННЫЕ КОМПЬЮТЕРНЫЕ СИСТЕМЫ

Предложен механизм локализации вторжений в распределенные компьютерные системы на основе специальных локальных и центрального агентов мониторинга безопасности. Разработан улучшенный алгоритм их взаимодействия. Проведены экспериментальные исследования параметров разработанных механизмов системы безопасности, которые подтвердили повышенную эффективность предложенных средств для выявления и ограничения потенциальных вторжений.

Ключевые слова: мониторинг, компьютерная система, безопасность, вторжение.

Введение. В настоящее время известен ряд систем обнаружения и локализации вторжений для классических компьютерных сетей, однако применение данных систем в классе распределенных компьютерных систем (РКС) достаточно ограничено, что вызывает необходимость адаптации существующих механизмов безопасности к особенностям функционирования РКС. Развитие коммуникационных технологий позволяет строить cloud-системы, объединяющие значительное число доменов, расположенных на значительном удалении друг от друга, что обуславливает рост числа узлов в данных системах и числа коммуникационных каналов связи, что, в свою очередь, расширяет возможность получения несанкционированного доступа к cloud-системе со стороны злоумышленников. [1,2]

Задачами систем обнаружения вторжений и мониторинга безопасности РКС является систематический сбор и обработка информации по событиям безопасности, при этом данная информация также используется при управлении безопасностью. В частности, данные системы позволяют выявлять критичные состояния РКС или подготовку к вторжению в данные системы. [3,4,5] Задачей статьи является реализация процедуры локализации вторжений в РКС, позволяющей эффективно и оперативно реагировать на факторы нарушения безопасности и нейтрализовать их.

Специализированные агенты для локализации вторжений в РКС. В качестве РКС рассмотрим систему, в которой на одном сервере может находиться несколько виртуальных локальных узлов, при этом в качестве центрального узла выступает отдельная рабочая станция. Данная система может масштабироваться как путем добавления новых серверов виртуализации, так и путем добавления виртуальных локальных узлов. Для реализации мониторинга безопасности каждого отдельного узла РКС разработан специальный агент сбора статистики по безопасности.

Предложенная распределенная система локализации вторжений состоит из центрального агента (ЦА) и локальных агентов (ЛА), размещенных на виртуальных узлах cloud-системы.

Структура предложенной системы локализации вторжений изображена на рис. 1.

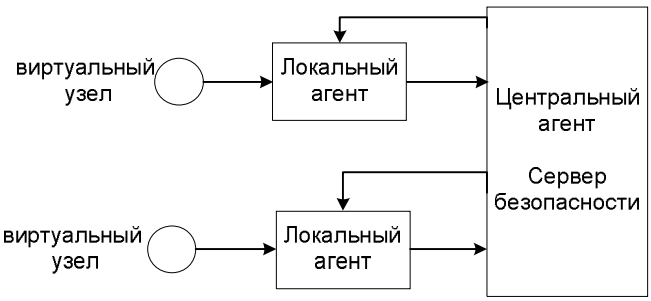

Рис. 1. Предложенная система специализированных агентов

Аппаратная часть и программное обеспечение ЛА поддерживает автономную защиту локального участка РКС, а также обнаруживает и анализирует все сессии виртуального узла. В случае если сессия оказывается атакой, ЛА собственными средствами защиты устраняет действия атаки, регистрирует данное событие, и информирует об этом ЦА. ЦА в свою

очередь анализирует полученную информацию, в случае необходимости отключает атакующие узлы и сообщает остальным ЛА о потенциальной угрозе.

Предложенный механизм является комплексным, он включает в себя два суб-агента: локальный агент, расположенный на каждом виртуальном локальном узле cloud-системы и центральный агент, расположенный на отдельном сервере. Локальный агент производит сбор статистики на локальном узле по запросам от центрального узла. Структура локального агента приведена на рис. 2. Он состоит из модуля сбора статистики, а также модуля связи с центральным агентом.

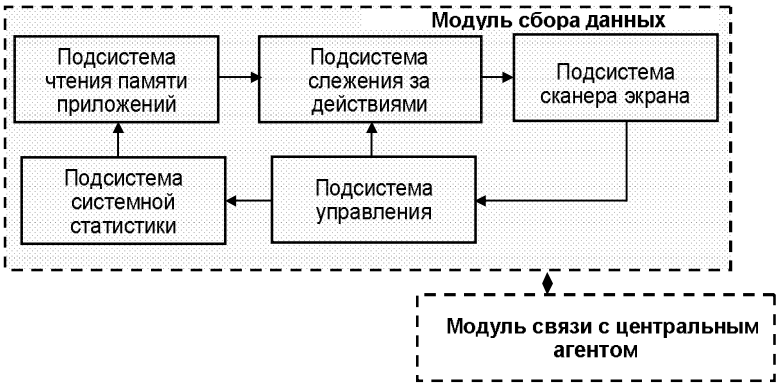

Рис. 2. Структура локального агента для обнаружения вторжений в РКС

Модуль сбора статистических данных включает в себя:
- Подсистему чтения памяти приложений;
- Подсистему слежения за действиями пользователя;
- Подсистему сканера экрана;
- Подсистему управления.

Подсистема чтения памяти приложений позволяет выполнять чтение из памяти любого приложения по указанным адресам в памяти. Данная подсистема позволяет отслеживать ключевые точки в памяти программы и системных служб с точки зрения их изменения.

Подсистема слежения за действиями пользователя выполняет действия по получению информации об открытых приложениях. Данная подсистема позволяет получить детальную статистику о том, какими программами пользуется пользователь, а также позволяет определить время доступа пользователя к файлу.

Подсистема сканера экрана позволяет сделать снимок экрана или снимок любой его части. Данная подсистема позволяет выявить появление окон, которые не смогла определить подсистема слежения за действиями пользователя, а также позволяет производить запись действия пользователя и в случае определённых ошибок воспроизвести последовательность действия, которая к ним привела.

Подсистема системной статистики позволяет выполнять сбор детализированной статистики по большинству системных параметров, таких как: количество открытых портов, количество запущенных процессов, объём свободной памяти, загруженность канала передачи данных и другие.

Подсистема управления позволяет выполнить удалённое управление локальным агентом с центрального агента. Подсистема управления может имитировать действия пользователя, например, путем перемещений курсора в заданную область, также блок позволяет удалённо запускать приложения.

Следует отметить, что локальный агент предназначен для сбора детализированной статистики и передачи информации на центральный узел, где и выполняется анализ полученных данных. Также локальный агент содержит специальный механизм для управления виртуальным узлом.

Подсистема связи с центральным агентом предназначена для формирования ответов на запросы от центрального агента. Ввиду того, что центральный узел посылает множество

запросов на локальные узлы, возникает проблема задержек получения данных от локальных узлов, связанная с ограничениями скорости передачи данных. Ввиду значительного числа запросов-ответов, вероятность внешнего воздействия на систему резко возрастает, а возможность отслеживания их корректности снижается.

Центральный агент, расположенный на отдельном сервере отвечает за вызов процедуры сбора детализированной статистики, её анализ, а также в случае выявления угроз реализует реакцию на них.

Центральный агент (рис. 3) состоит из:

- Модуля связи с локальными агентами;
- Подсистемы сохранения статистики;
- Подсистемы управления локальными агентами;
- Подсистемы анализа статистики;
- Подсистемы локализации вторжений.

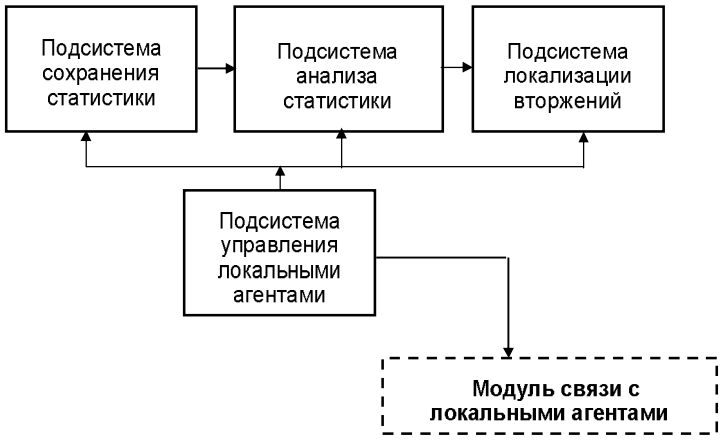

Рис. 3. Центральный агент сбора статистики и локализации вторжений в РКС

Центральный агент выполняет периодический опрос локальных агентов. Под опросом понимается формирование запроса на получение статистики по определённым параметрам, в качестве параметров выступает тип проверки (чтение памяти приложений, получение загрузки локального агента, запрос на получение другой статистики). Сформированный запрос передаётся для обработки на локальный агент.

Подсистема формирования запросов представляет собой набор средств, которые позволяют осуществлять периодические проверки состояния локальных агентов. Данная подсистема содержит базу данных проверок, которую администратор может пополнять, и которая имеет следующий формат:

Проверка - Время первого запуска проверки - Периодичность перезапуска проверки – Соседние узлы.

Подсистема формирования запросов просматривает все доступные проверки из базы данных проверок и определяет, наступило ли время на запуск проверки, и если время наступило, то проверка запускается.

Подсистема связи с локальными агентами предоставляет средства для подключения или отключения локальных агентов. Данная подсистема также предназначена для проверки подключённых агентов на доступность, в качестве локальных агентов может выступать несколько виртуальных машин на одном сервере, в таком случае для каждой виртуальной станции выдаётся отдельный порт, через который локальный агент осуществляет связь с центральным агентом. Проверка локальных агентов на доступность происходит периодически и инициируется центральным агентом, что позволяет исключить подключения к cloud-системе ложных агентов.

Подсистема анализа статистики и подсистема локализации вторжений (ПЛВ) осуществляют анализ данных полученных от блока формирования опросов, который также

содержит базу данных реакций. Под реакцией понимается набор действий, которые выполняются в ответ на определённые действия.

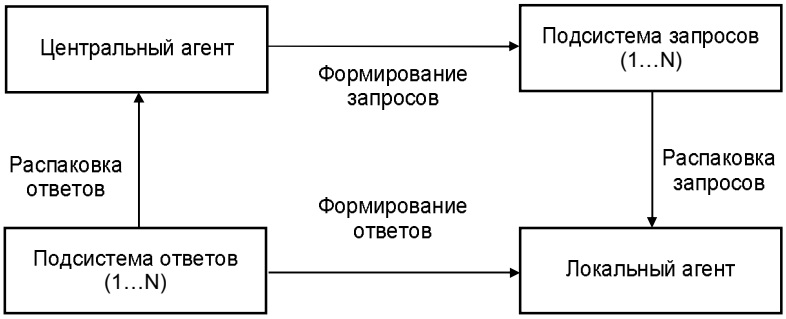

Рис. 4. Механизм обмена данными центрального и локального агентов

Для снижения времени задержек получения данных, увеличения удельного объема полезной информации и повышения безопасности cloud-системы предлагается механизм объединения однотипных запросов от центрального агента в единый пакет. Пакет с запросами поступает на локальный агент, на котором он распаковывается, после чего локальный агент собирает ответы на каждый запрос в блоке и формирует пакет ответов, который передаётся на центральный агент. Применение такого механизма позволяет уменьшить задержки и увеличить объём полезного трафика. Механизм обмена данными изображен на рис. 4. В случае реагирование на потенциальное вторжение, в том числе путем локализации опасных узлов, для уменьшения времени реакции объединение в пакеты не выполняется.

Предложенный механизм локализации вторжений в распределенные компьютерные системы на основе специальных локальных и центрального агентов обладает рядом преимуществ:

- обнаружение вторжений на локальном уровне;
- анализ вторжений на узле;
- оперативное отключение атакующих субъектов;
- возможность обратной связи ЛА с ЦА;
- понижение загруженности ЦА;
- предотвращение атак на других узлах РКС.

Постановка и проведение экспериментальных исследований. Структура системы сбора информации. В качестве системы для сбора статистики использован комплекс из 4-х локальных субъектов и одного сервера безопасности, при этом два из четырёх локальных агентов расположены на одной рабочей станции. Схема данного комплекса сбора информации изображена на рис. 5.

В процессе сбора статистических данных формируется специальный сеансовый вектор X = $\{x_1, x_2,\ldots, x_n\}$, содержащий те факторы (действия пользователей и приложений), которые потенциально могут быть связаны с нарушением безопасности системы. В частности, элементами вектора X являются следующие факторы:

- x_1: запущенные системные процессы;
- x_2: интегральное время недоступности агента (в мин);
- x_3: открытые порты;
- x_4: удельный объём занятой памяти (в %);
- x_5: показатель соотношения времени доступа к файлу и его размера (мс/Кб);
- x_6: показатель загруженности канала передачи данных (в %);
- x_7: потенциально опасные программы, в т.ч. на соседних узлах.

Для каждого фактора вектора X устанавливается весовой коэффициент его влияния на безопасность системы. Значения коэффициентов представлены в табл 1.

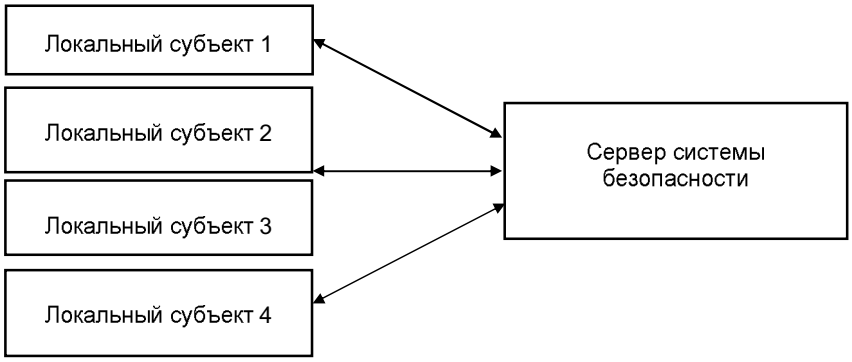

Рис. 5. Подсистема локализации вторжений для проведения экспериментов

Весовые коэффициенты опасности действий субъектов Таблица 1

ω_1	ω_2	ω_3	ω_4	ω_5	ω_6	ω_7
0.05	0.15	0.15	0.1	0.20	0.1	0.25

Далее, формируется пороговый вектор X_{max}, содержащий в качестве элементов x_{imax} максимально допустимые значения соответствующего фактора, при котором данное действие пользователя еще не является вторжением. Эти значения представлены в табл. 2.

Пороговые значения сеансового вектора Таблица 2

X_{1MAX}	X_{2MAX}	X_{3MAX}	X_{4MAX}	X_{5MAX}	X_{6MAX}	X_{7MAX}
80	1	7	70	5	30	0

Сбор детализированной статистики по каждому из четырёх субъектов проведен по трем сеансам работы в системе длительностью 20 мин каждый. Сформирована статистика 2-х видов: в первом эксперименте проводился сбор статистики без локализации вторжений, а во втором – с использованием подсистемы локализации вторжений. Для генерации данных по вторжениям использовалась имитационная модель нарушителя.

Экспериментальные исследования. В табл. 3 и табл. 4 представлены статистические результаты действий локальных субъектов 2 и 3 без использования локализации вторжений.

В табл. 5 и табл. 6 представлены статистические результаты действий на локальных субъектах 2 и 3 с использованием ПЛВ.

Статистика действий локального субъекта 2 без использования ПЛВ Таблица 3

Время (мин.)	x_1	x_2	x_3	x_4	x_5	x_6	x_7	P
5	83	0	6	64	0	6	0	0,05
10	84	0	6	63	0	7	0	0,05
15	82	0	8	65	0	7	0	0,2
20	83	0	8	61	1,70	5	0	0,2
25	94	0	10	63	0	8	0	0,2
30	93	2	12	61	0	8	0	0,35
35	95	0	11	62	0	34	1	0,55
40	96	0	15	63	0	5	1	0,45
45	98	0	6	60	2,10	11	0	0,05
50	97	0	6	71	0,00	11	0	0,15
55	103	0	7	69	25,60	9	1	0,5
60	102	2	6	72	0,00	8	0	0,3

Статистика действий локального субъекта 3 без использования ПЛВ Таблица 4

Время (мин.)	x_1	x_2	x_3	x_4	x_5	x_6	x_7	P
5	76	0	6	68	6,80	8	0	0,2
10	73	0	8	66	0,00	6	0	0,15
15	75	2	6	69	2,00	13	0	0,15
20	72	0	7	71	3,00	15	0	0,1
25	74	1	7	82	0,00	14	0	0,1
30	71	3	6	81	0,00	16	0	0,25
35	76	0	7	86	2,40	17	0	0,1
40	81	0	8	78	1,00	22	0	0,3
45	83	0	6	67	2,00	7	1	0,3
50	79	0	7	66	10,20	42	0	0,3
55	78	0	7	72	0,00	12	1	0,35
60	81	0	8	75	0,00	24	0	0,3

Статистика действий локального субъекта 2 с использованием ПЛВ Таблица 5

Время (мин.)	x_1	x_2	x_3	x_4	x_5	x_6	x_7	#2
5	83	0	6	64	0	6	0	0,05
10	84	0	6	63	0	7	0	0,05
15	82	0	8	65	0	7	0	0,2
20	83	0	8	61	1,70	5	0	0,2
25	94	0	10	63	0	8	0	0,2
30	93	2	12	61	0	8	0	0,35
35	95	0	11	62	0	34	1	0,55
40	0	0	0	0	0	0	0	0
45	0	0	0	0	0	0	0	0
50	0	0	0	0	0	0	0	0
55	0	0	0	0	0	0	0	0
60	0	0	0	0	0	0	0	0

Статистика действий локального субъекта 3 с использованием ПЛВ Таблица 6

Время (мин.)	x_1	x_2	x_3	x_4	x_5	x_6	x_7	#3
5	76	0	6	68	6,80	8	0	0,2
10	73	0	8	66	0,00	6	0	0,15
15	75	2	6	69	2,00	13	0	0,15
20	72	0	7	71	3,00	15	0	0,1
25	74	1	7	82	0,00	14	0	0,1
30	71	3	6	81	0,00	16	0	0,25
35	76	0	7	86	2,40	17	0	0,1
40	81	0	8	78	1,00	22	0	0,3
45	0	0	0	0	0	0	0	0
50	0	0	0	0	0	0	0	0
55	0	0	0	0	0	0	0	0
60	0	0	0	0	0	0	0	0

На рис. 6 и рис. 7 предоставлены графические зависимости, построенные по данным таблиц 3 - 6.

Рис. 6 и 7 показывают, что, в отличие от варианта, когда подсистема локализации вторжений не использовалась, при ее использовании в случае обнаружения потенциальной угрозы проводилось отключение соответствующего локального субъекта, а также снижался допустимый уровень угроз на смежном субъекте, при достижении которого он также был отключён. В результате оказалось, что все возможные повторные угрозы были нейтрализованы.

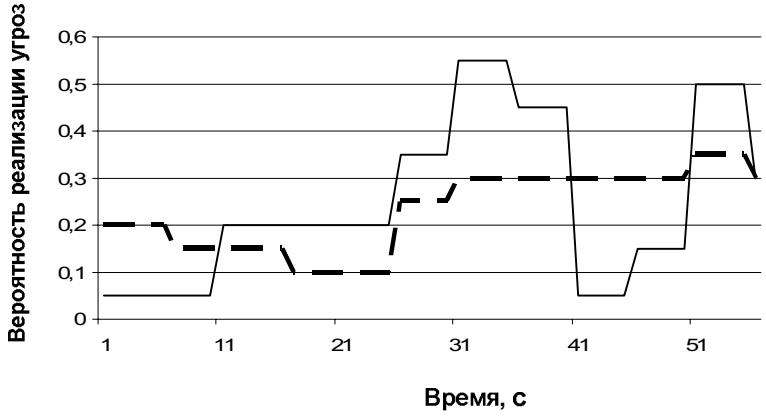

Рис. 6. Статистика действий локальных субъектов 2 и 3 без использования ПЛВ (сплошная линия – субъект 2, пунктирная – субъект 3)

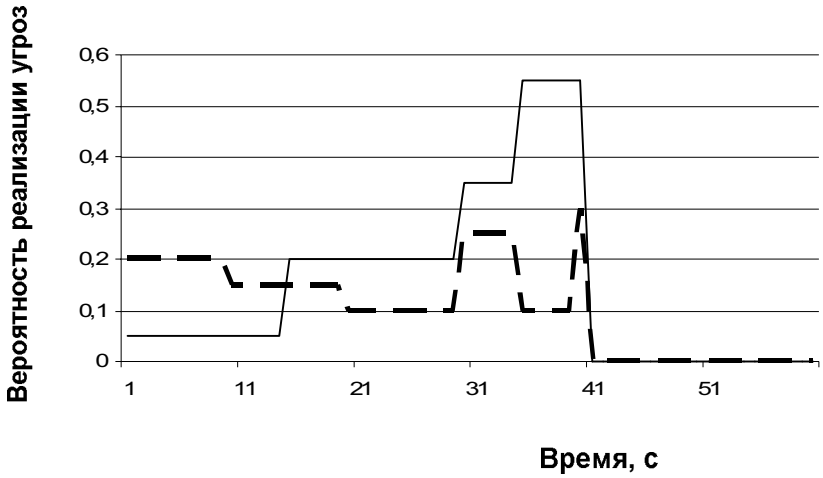

Рис. 7. Статистика действий локальных субъектов 2 и 3 с использованием ПЛВ (сплошная линия – субъект 2, пунктирная – субъект 3)

При проведении следующего эксперимента задействованы десять локальных субъектов, которые производили имитацию различных, в т.ч. несанкционированных, действий. В частности, отдельные действия пользователей были направлены на превышение пороговых значений вектора X. Результаты представлены на рис. 8.

Как показывает рис. 8, количество реализованных атак в случае не использования подсистемы принятия решений оказалось выше в 3.4 раза по сравнению с использованием данной подсистемы, так как на основе решения ПЛВ выполнялось отключение локальных субъектов, генерирующих атаки.

Заключение. Проблема защиты распределенных компьютерных систем от несанкционированного доступа имеет особенную актуальность. В работе предложены структурные компоненты системы безопасности РКС, реализованные в виде локального и центрального агентов мониторинга безопасности, а также разработан механизм их взаимодействия и локализации вторжений.

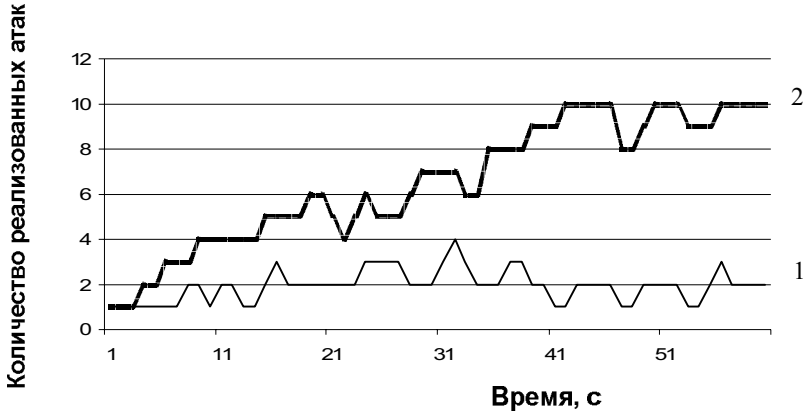

Рис. 8. Количество реализованных атак в cloud-системе с использованием (1) и без использования (2) ПЛВ

Представлены особенности реализации локального и центрального агентов системы локализации вторжений в РКС, а также их основные функции. Проведены экспериментальные исследования параметров разработанной системы, которые показали, что предложенные агенты позволяют эффективно выявлять потенциальные атаки и оперативно отключать атакующие локальные субъекты от cloud-системы, что обеспечивает снижение общего число атак и потенциально опасных угроз.

ЛИТЕРАТУРА

1. Широчин В.П., Широчин С.В, Мухин В.Е. Основи безпеки комп'ютерних систем. Київ «Корнійчук», 2009. – 290 с.

2. Badger Lee, Grance Tim, Patt-Corner Robert, Voas Jeff. DRAFT Cloud Computing Synopsis and Recommendations Special Publication 800-146, May 2011.

3. Гатчин Ю.А. Основы информационной безопасности: учебное пособие/ Ю.А. Гатчин, Е.В. Климова. – СПб.: СПбГУ ИТМО, 2009. – 84с.

4. Завгородний В.И. Комплексная защита в компьютерных системах / В.И. Завгородний. – М.: Логос, 2001. – 264 с.

5. Hubbard Dan, Sutton Michael etc. Top Threats to Cloud Computing V1.0. Cloud Security Alliance, March 2010.

Надійшла: 02.09.2012р.

Рецензент: д.т.н., проф. Розорінов Г.М.