МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное

образовательное учреждение высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт

Факультет	*Кафедра*
вычислительной техники	Высшая и прикладная математика
(наименование)	(наименование)

Направление подготовки 01.03.04 «Прикладная математика»
(код и наименование)

Профиль Математическое моделирование в экономике и технике
(код и наименование)

БАКАЛАВРСКАЯ РАБОТА

на тему

ВОПРОСЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

Студент 17ВВ1 (группа) — 17.06.21 (подпись, дата) — Мысякин И. С. (фамилия, инициалы)

Руководитель к..ф.-м.н, доцент — 17.06.21 (подпись, дата) — Захарова Ю. Ф. (фамилия, инициалы)

Нормоконтролер к.т.н., доцент — 17.06.21 (подпись, дата) — Тарасов Д. В. (фамилия, инициалы)

Работа допущена к защите (протокол заседания кафедры от 04.06.2021г. № 10)

Заведующий кафедрой д.ф.-м.н., проф. — 18.06.21 (подпись, дата) — Бойков И. В. (фамилия, инициалы)

Работа защищена с отметкой отл. (протокол заседания ГЭК от 22.06.21г. № 4)

Секретарь ГЭК к.пед.н., доцент — 22.06.21г. (подпись, дата) — Зверовщикова Н. В. (фамилия, инициалы)

Пенза 2021

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное

образовательное учреждение высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт

Факультет

Вычислительной техники
(наименование)

Кафедра

Высшая и прикладная математика
(наименование)

«УТВЕРЖДАЮ»

Заведующий кафедрой

И. В. Бойков
(подпись, инициалы, фамилия)

«30» ноября 2020 г.

ЗАДАНИЕ

на бакалаврскую работу

1. Студент Мысякин Илья Сергеевич гр. 17ВБ1
(фамилия, имя, отчество)

факультета вычислительной техники

2. Тема работы Вопросы защиты информации при использовании облачных технологий

Тема утверждена приказом по ПГУ № 0903_о от « 30 » ноября 2020 г.

3. Руководитель работы к.ф.-м. н., доцент Захарова Ю. Ф.

4. Задание на работу (назначение разработки, исходные данные и т.п.)

1. Исследовать текущее состояние вопроса о опасностях и мерах противодействия им в облачных системах

2. Изучить современные методы противодействия различным угрозам информационной безопасности облачных распределенных систем

3. Построить математическую модель системы безопасности облачной системы для оптимизации размещения средств защиты информации

4. Выполнить программную реализацию разработанной модели

5. Привести сравнительную оценку нанесенного ущерба облачной системе

5. Перечень подлежащих разработке вопросов

1. Провести анализ современных методов противодействия различным угрозам информационной безопасности облачных распределенных систем

2. Провести выбор используемых при защите облачной системы программных комплексов для каждого вида угроз информационной безопасности

3. Построить математическую модель облачной системы, провести её программную реализацию и выполнить решение модельной задачу

4. Сформулировать выводы о построенной математической модели и возможности её применения в различных облачных системах

6. Календарный график по выполнению проекта

Наименование этапов работы	Объем работы	Срок выполнения	Подпись руководителя
1. Обзор литературы	20 %	28.05.2021	
2. Исследование методов защиты с применением облачных технологий	25 %	02.06.2021	
3. Построение математической модели распределённой облачной системы	20 %	07.06.2021	
4. Разработка программы	25 %	10.06.2021	
5. Оформление пояснительной записки	10 %	14.06.2021	

Дата выдачи задания « 30 » ноября 2020 г.

Руководитель бакалаврской работы _____ Ю.Ф. Захарова
(подпись, инициалы, фамилия)

Задание к исполнению принял студент _____ И. С. Мысякин
(подпись, инициалы, фамилия)

Работу к защите допустить
Декан факультета _____ Л. Р. Фионова
(подпись, инициалы, фамилия)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 4
1. АНАЛИЗ АРХИТЕКТУРЫ И ОРГАНИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННЫХ ОБЛАЧНЫХ СИСТЕМ 8
1.1. Архитектура информационной безопасности облачных систем 8
1.2. Анализ технологии и структуры облачной среды 11
1.3. Анализ вариантов построения облачных сред и размещения в них средств защиты информации 14
1.4. Алгоритмы шифрования применяемые в распределенных облачных системах 22
1.4.1. PP-CP-ABE -шифрование 22
1.4.2. Настройка системы и ключа 23
1.4.3. Аутсорсинговое PP-CP-ABE шифрование 24
1.4.4. Алгоритм дешифрования 25
2. МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОБЛАЧНОЙ СИСТЕМЫ 28
2.1. Построение модели угроз информационной безопасности для распределенной облачной системы. 28
2.2. Элементы оптимальной модели облачной системы 33
2.3. Проблема оптимизации структуры информационной безопасности для облачных систем 38
2.4. Построение оптимальной по затратам и ущербу модели распределённой облачной системы 41
3. ПРОГРАММНАЯ РЕАЛИЗАЦИЯ РАЗРАБОТАННЫХ МОДЕЛЕЙ И ИХ ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ ДЛЯ ПРОЕКТИРОВАНИЯ АРХИТЕКТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЛАЧНЫХ СИСТЕМ 47

3.1. Программная реализация инструментария для построения и исследования архитектуры информационной безопасности облачных систем 47
3.2. Пример расчёта оптимального варианта размещения средств защиты в облачной системе 49
ЗАКЛЮЧЕНИЕ 54
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 55
ПРИЛОЖЕНИЕ А. Листинг программы 59

ВВЕДЕНИЕ

Актуальность проблемы. Начиная с середины прошлого века, когда началось активное развитие информационных технологий, применение их во всех областях жизнедеятельности стало лишь вопросом времени. В настоящее время не найти ни одной компании которая бы в своем процессе управления и производства не применяла бы вычислительные средства. Так как многие кампании и предприятия обладают филиалами в разных городах и даже странах возникает необходимость в использовании распределенных информационных систем. Современным подходом в этой области является использование распределенных облачных систем. Данный подход заключается в использовании ресурсов вычислительной сети как интернет сервис. Особенностью облачных систем является, то, что ресурсы, используемые пользователем облака, являются динамическими, а архитектура облака и используемые в нем узлы скрыта от пользователей. Также облачные системы, по своей сути являются аутсортинговыми услугами, что позволяет экономить средства на аппаратной и программной части распределенной системы. Высокая надёжность, доступность, простота использования и возможность широкой настройки облачной системы под необходимую задачу делают их перспективным вариантом реализации распределённых информационных систем. Поэтому, поддержание информационной безопасности, соответствующей требуемому уровню качества, является одной из первостепенных задач, стоящих перед проектировщиками сетевой инфраструктуры. Исследованиям по системному анализу и оценке угроз рисков информационной безопасности и средств защиты были посвящены работы следующих авторов: Гайдамакин Н. А. [1], Скиба В. Ю. [2], Богаченко Н. Ф. [3], Гильмуллин Т. М. [4], Ширинкин М. С. [5], Голембиовская О. М. [6], Моляков А. С.[7], Асмолов М. А.[8]. Скиба В. Ю. [2] предлагает подход, связанный с классификацией угроз безопасности, и рассматривает возможности разработки системы международной информационной безопасности. Богаченко Н. Ф.[3] в своих работах предлагает прецедентный подход к построению политики ин-

формационной безопасности. В рекомендациях NIST подробно описана архитектура, основные уязвимости и особенности облачных систем. Данные работы рассматривают различные аспекты информационной безопасности, однако в настоящий момент не существует универсального подхода, способного предоставлять оптимальный вариант размещения средств защиты информации на основании заданной архитектуры сети, анализа механизмов информационной безопасности и их эффективности относительного имеющегося спектра угроз. Как следствие, встаёт вопрос о создании такого подхода, который должен иметь следующие отличительные особенности:

1. Построение универсальной методики на основе концептуальной модели распределённой системы обработки информации для оптимизации размещения средств защиты;

2. Возможность проектирования архитектуры информационной безопасности, исходя из структуры конкретной распределённой сети;

3. Системный анализ угроз, возникающих на каждом элементе сети, таких как сетевое оборудование, серверы облачной системы, локальные компьютеры и мобильные устройства пользователей;

4. Возможность выбора средств защиты по противодействию конкретной угрозе из разных классов, что позволит отразить эквивалентность механизмов информационной безопасности;

Использование системного подхода позволит при проектировании и управлении информационной безопасностью учесть большинство факторов, оказывающих влияние на информационную защищённость системы, и получить обоснованные рекомендации по размещению механизмов информационной безопасности на основании конкретной архитектуры вычислительной сети.

В связи с вышеизложенным можно сделать вывод, что исследования в этой области являются целесообразными, а тема данной научной работы - актуальна.

Объектом исследования являются распределённые системы с использованием облачных вычислений.

Предметом исследования являются модели и алгоритмы оптимального размещения средств защиты информации, позволяющего сформировать комплекс средств противодействия угрозам нарушения информационной безопасности в распределённых облачных системах.

Целью бакалаврской работы является разработка математической модели распределённой информационной системы и алгоритма принятия решения по оптимизации размещения средств защиты информации.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Выполнить анализ существующих моделей и технологий построения архитектуры информационной безопасности распределённых систем;

2. Разработать математическую модель распределённых информационных систем, учитывающую особенности облачных технологий и основанную на системном подходе к оптимизации размещения средств защиты информации;

3. Разработать модифицированные алгоритмы принятия решения по выбору оптимального размещения средств защиты информации в распределённых системах;

4. Исследовать механизмы и средства обеспечения информационной безопасности в распределённых системах на базе вычислительных сетей и в рамках технологии облачных вычислений;

5. Выполнить на основе методов системного анализа классификацию и оценку угроз информационной безопасности и мер противодействия им на основе имеющихся данных об информационной сети;

6. Разработать программное обеспечение, реализующее предложенные модели и алгоритмы оптимизации размещения средств защиты информации в распределённых системах.

Научная новизна работы заключается в том, что:

1. Разработана математическая модель распределённой системы для решения задачи оптимизации размещения средств защиты информации, отличающаяся от известных моделей тем, что основана на системном анализе архи-

тектуры вычислительной сети и угроз. Модель позволяет заменять средства защиты из одного класса средствами из другого класса, если они выполняют сходные функции;

2. Разработано программное обеспечение, позволяющее принять обоснованное решение по оптимальному размещению средств защиты информации, что позволяет сформировать структуру информационной безопасности распределённой системы на основании заданных архитектуры сети и набора средств защиты информации;

Теоретическая ценность и практическая значимость. Результаты исследований, представленные в работе, могут быть использованы в различных областях науки и техники. Так, предложенная математическая модель распределённой системы для оптимизации размещения средств защиты информации может быть применена при решении задач оптимального размещения и многокритериальной оценке.

Разработанное программное обеспечение может применяться при проектировании информационной безопасности.

Методы исследования и достоверность результатов. В работе использованы методы системного анализа, методы решения комбинаторных задач, методы теории принятия решений и имитационного моделирования, методы экспертного оценивания, элементы теории вероятностей, генетические и муравьиные алгоритмы. Достоверность научных результатов и выводов подтверждается обоснованным применением математического аппарата; совпадением полученных результатов решения задачи принятия решения по размещению средств защиты информации с использованием генетических алгоритмов и точных методов.

1. АНАЛИЗ АРХИТЕКТУРЫ И ОРГАНИЗАЦИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННЫХ ОБЛАЧНЫХ СИСТЕМ

1.1. Архитектура информационной безопасности облачных систем

Информационная безопасность распределенной облачной системы, это состояние элементов облачной системы, которое позволяет поддерживать заданный уровень защиты от возможных случайных или преднамеренных угроз естественного или искусственного характера.

Недопуск возникновения ущерба объектам распределенной системы, захватывая и её пользователей, является основной целью защиты информации.

Система защиты должна содержать следующие характеристики:

– обеспечение конфиденциальности;

– легкость использования;

– сохранение исходного состояния данных.

Информационный процесс, информация или её носитель могут являться объектом защиты.

Механизмы защиты - объединение средств защиты информации (СЗИ), во время совместного функционирования и решения поставленных задач по защите информации являются системой обеспечения безопасности данных.

В следствии того что, существует множество возможных средств и методов решения задачи по защите информации данной распределенной системы, появляется проблема выбора максимально удовлетворяющей всем требованиям в заданных границах для решения поставленной задачи, что требует соответствующие изменения в выборе оптимальной структуры, режимов работы системы, определенных мест расположения элементов распределенной облачной системы и т.д.

Процесс построения информационной безопасности должен включать меры по обнаружению и противодействию возможных угроз, вызывающих негативные последствия для системы. Угроза может затрагивать как всю си-

стему, так и отдельные её части. После обнаружения угрозы система безопасности должна выбрать способ защиты, направленный на выявленную угрозу и средства защиты выполняющие функции, использующие соответствующие методы.

Чтобы эффективно поддерживать требуемый уровень информационной безопасности необходимо использовать современные механизмы защиты от различных видов угроз облачной системе. Подобные механизмы защиты должны включать в себя аппаратные, программные и организационные уровни защиты. Так как в настоящее время многие кампании занимаются методами определения и противодействия различным угрозам для информации, то соответственно существует большое количество различных методов организации процесса информационной защиты при проектировании защиты нужно учитывать различные вариации построения архитектуры системы информационной безопасности, доступные аппаратные и программные средства, а также взаимосвязь между собой различных средств безопасности. Объединение различных механизмов защиты информации в единую систему позволяет улучшать характеристики отдельных средств защиты, а также создает новые возможности для обнаружения и противодействия как новым угрозам, так и новые методы противодействия для известных угроз. Поэтому задача оптимизации информационной безопасности заключается в подборе средств защиты для обеспечения максимального уровня информационной безопасности при заданных условиях (стоимость, архитектура облачной системы, уровень защиты и д. р.), среди различных механизмов защиты, имеющих эквивалентные методы защиты.

Как уже было отмечено, средства обеспечения информационной безопасности делятся на:

- программные;
- аппаратные;
- организационные.

Программными средствами являются такие механизмы защиты как проверка и обеспечение доступа к системе в целом или её частям, методы шифро-

вания хранящейся в ядре облачной системы и передаваемые как внутри системы так и во вне, а также многие другие средства. Достоинством программных средств защиты является доступность, простота установки и использования, постоянное развитие и возможность модификации практически без какого-либо участия специалистов по информационной безопасности и системных администраторов. К недостаткам можно отнести потребность в использовании части ресурсов системы, высокая чувствительность к изменению архитектуры и аппаратного состава облачной системы.

Аппаратными средствами защиты являются различные электронные и электронно-оптические устройства, обеспечивающие какой-либо из механизмов информационной безопасности, такие как различные устройства для идентификации пользователей, шифрования передаваемых данных и многие другие. Их достоинством является надежность, недоступность для атаки из вне, устойчивость к изменениям архитектуры и аппаратного состава системы. Недостатками же является их стоимость, невозможность, в большинстве случаем, их модификации, сложность установки, а также занимаемое место и масса.

Организационными средствами являются различные мероприятия, проводящиеся в течении всего цикла жизни облачной системы среди обслуживающего персонала и пользователей этой системы.

С момента своего появления облачные технологии все более и более интегрируются в сферу распределенных систем. Это происходит, в связи с тем, что многие кампании являются территориально распределёнными и создавать таким компаниям свою собственную распределенную систему невыгодно. И появление облачных провайдеров, а также возможности арендовать облачный сервер (или его часть) вместе с уже существующей системой безопасности позволяет таким кампаниям осуществлять свою работу, несмотря на местоположение своих отделений и сотрудников. К тому же в большинстве случаев аренда облачной системы будет гораздо выгоднее экономически, в связи с тем, что не придется закупать оборудование и держать в штате специалиста по информационной безопасности. Так как далеко не все предприятия могут позволить се-

бе арендовать целое облако, данные многих компаний хранятся в одном и том же «облаке». Поэтому из-за широкого распространения облачных систем появляются обязательные требования к поддержанию информационной безопасности данных, хранимых в этих системах. Это требует достаточно строгого механизма разграничения доступа к различным данным, хранящимся в облачном сервере. Также так как, передача данных идет через интернет (т.е. по незащищенному каналу) то для облачных систем требования к шифрованию являются более строгими.

1.2. Анализ технологии и структуры облачной среды

Облачные вычисления – это модель предоставления общего сетевого доступа по запросу к общему пулу вычислительных ресурсов, при котором у пользователя имеется только доступ к интерфейсу облачной системы, позволяющему обращаться к облачной системе, а вся информация клиента, так же как и применяемое им программное обеспечение находится на стороне провайдера.

К преимуществам облачных вычислений относятся:

– Доступность;

– Низкая стоимость;

– Гибкость;

– Надежность;

– Большие вычислительные мощности и возможность быстрого их наращивания;

– Высокая информационная безопасность облачных серверов.

Так же, рассматривая классические структуры хранения информации, можно отметить, что лишь маленькое число организаций, за исключением крупных, обладают собственной политикой информационной безопасности. Кроме того, её внедрение иногда оставляет желать лучшего, а внутренняя защита информации не построена необходимым образом. Из этого следует, что хранение информации в «облаке» и обеспечение её надлежащей защиты выглядит более выгодно, чем офисная структура, где данные находятся не в определенном ме-

сте, а рассредоточены по различным рабочим станциям и филиалам. К тому же в соглашении с облачным провайдером часто указываются нормы и условия, которые касаются информационной безопасности, при нарушении которых провайдер понесет финансовую ответственность.

Недостатками облачных систем является:

1. Нуждаемость непрерывного подключения к сети интернет;

2. Наличие ограничений на применяемое программное обеспечение и его корректировку под нужды клиента;

3. Конфиденциальность информации – на данный момент не существует технологии обеспечивающей полную безопасность информации. На ряду с тем вопрос недоступности данных для посторонних лиц является одним из главных в облачных системах, ведь при низкой степени защиты «облака» появляется возможность проникновения в систему и получения доступа как к данным любого человека хранящего информацию в этом облаке, так и к возможности модификации облачной структуры, злоумышленником обладающим доступом к сети Интернет и находящимся практически в любой точке мира;

4. Высокая стоимость создания личного облака для малых организаций, которое может затребовать большое число финансовых вложений;

Не взирая на то, что «облака» остаются достаточно защищенными структурами, имеется ряд проблем, относящихся к безопасности содержащихся на них данных:

а) технологические и материальных нюансы, связанные со слабостями, типичными для сетевых структур;

б) психологические проблемы, относящиеся к малому уровню доверия к новой лишь набирающей широкое распространение области, каковой являются облачные системы;

в) юридические аспекты – в Европе и Америке ещё с конца прошлого века были разработаны стандарты операционного аудита облачных систем. Набольшее распространение до 2011 получили стандарты SAS 70 Type II [9] и ISO 27001 [10], и в 2011 году они были заменены более совершенным стандар-

том SSAE 16. К сожалению, в России законодательная база, касающаяся безопасности облачных систем только начала своё развитие. Например, лишь в середине 2011 года был принят закон для защиты персональных данных граждан РФ №152-ФЗ «О персональных данных» [11]. Его развитие в виде закона о дополнительной защите персональных данных россиян было принято в декабре 2020 года и вступило в силу 1-го марта 2021 года.

Непосредственно для облачной обработки данных были созданы проекты ГОСТ «Защита информации. Требования по защите информации, обрабатываемой с использованием технологии виртуализации. Общие положения» [12] и «Требования по защите информации, обрабатываемой с использованием технологий «облачных вычислений» [13]. На данный момент действующим является только 2-й проект.

Опишем существующие типы облачных систем [14]:

1. Публичное облако – платформа, предоставляющая доступ пользователям через интернет. Пользователи арендуют вычислительные мощности и объем хранимых данных. Вся инфраструктура облака принадлежит провайдеру. За частую множество пользователей используют для обработки данных и хранения информации одно и тоже облако [15];

2. Частное облако – платформа, зачастую применяемая одной компанией или группой связанных компаний. В частном облаке аппаратная инфраструктура принадлежит предприятию и размещается в собственном дата-центре. Однако, к частным облакам также относят облака, созданные в арендованных помещениях, дата-центров провайдера или полная аренда облака у провайдера (но в этом случае доступ к облаку имеет лишь сама компания, арендовавшая её и те, кому эта компания доступ предоставит);

3. Гибридное облако – платформа, сочетающая в себе как частное, так и публичное облако. В случае нехватки ресурсов частного облака или для повышения уровня устойчивости к различным катастрофам может арендоваться дополнительные ресурсы публичного облака.

Существует несколько моделей развертывания облачных систем. Они отличаются друг от друга по функционалу, к которому получают доступ конечные пользователи. Наиболее часто встречающимися являются следующие модели обслуживания облачных систем [16]:

1. Программное обеспечение как услуга (SaaS) – модель, которая позволяет клиенту использовать только то программное обеспечение, которое расположено провайдером на облачном сервере. Считается самой безопасной моделью обслуживания облачной системы, в связи с тем, что остальные модели позволяют использовать в облачной системе практически любое программное обеспечение;

2. Платформа как услуга (PaaS) – модель, позволяющая клиенту располагать в облаке личное программное обеспечение.

3. Инфраструктура как услуга (IaaS) –модель, при которой провайдер предлагает пользователю возможность самому определиться архитектуру необходимой ему облачной системы, т.е. предлагает различные элементы облачной системы (сервера, хранилища данных, сетевые ресурсы и программное обеспечение) как услуги, которые пользователь может подключить или отключить в любой момент времени. К недостаткам этой модели можно отнести то, что данная модель по сравнению с моделью PaaS обладает несколько меньшей производительностью.

В 2004 году был принят стандарт Application Package Standard (APS) [17] направленный на улучшение безопасности облачных систем. Этот стандарт регулирует процесс построения программного обеспечения, которое может применяться в облачных системах.

1.3. Анализ вариантов построения облачных сред и размещения в них средств защиты информации

Существует несколько моделей построения облачных вычислений. Приведем наиболее популярные из них.

1. По версии NIST идеальная модель облачных вычислений формируется из пяти главных участников: облачный потребитель, облачный провайдер, аудитор облака, облачный блокер, облачный оператор связи [18]. Эта модель показана на рисунке 1.1.

Эта модель информационной системы облачных технологий (ИСОТ) состоит из нескольких уровней: уровень оркестрации, уровень сервиса, уровень абстракции и контроля за ресурсами, уровень материальных ресурсов.

Рисунок. 1.1 – Эталонная модель ИСОТ по версии NIST

Облачный сервис-менеджмент объединяет в себе все связанные с сервисом функции и возможности, необходимые для управления, функционирования и использования сервисов конечными пользователями облака;

2. Идеальная модель облачной системы, предложенная компанией Microsoft, подразделяется на три уровня:

- уровни программного обеспечения, платформы и инфраструктуры;
- оперативный уровень и уровень управления;
- уровень предоставления услуг.

Эти идеальные модели ИСОТ не детализируют уровни виртуализации сервисов. Поэтому, приведём модель, которая это делает. В работе [19] постро-

ена модель ИСОТ которая выделяет два главных субъекта облачных систем: пользователь облака и оператор облака.

В этой работе выделяются пять уровней облачной системы: уровень доступа, уровень виртуализации, уровень сервисов, уровень материальных ресурсов, уровень безопасности.

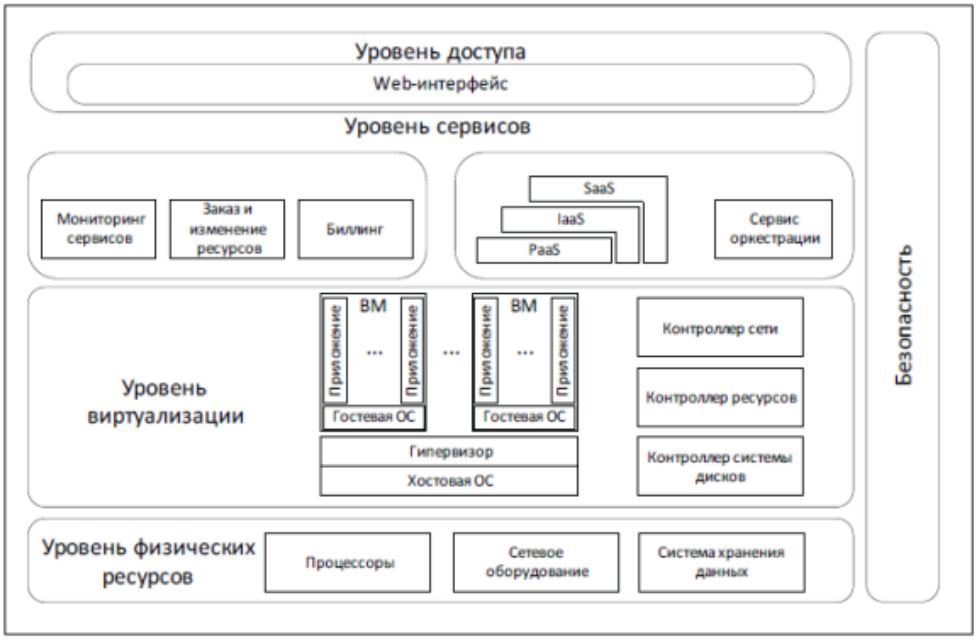

Рисунок 1.2 – Предложенная в работе [19] модель ИСОТ

Все облачные системы начинаются с организации их физической среды. Она используется для хранения данных, виртуализации сервера с помощью гипервизора и последующего предоставления доступа к виртуальным ресурсам пользователям. Структура облачной платформы приведена на рисунке 1.3.

Все выше указанные компоненты облачной системы могут подвергаться воздействию угроз информационной безопастности системы.

Со стороны информационной защиты можно отметить некоторые особенности облачных вычислений:

- размещение данных у провайдера;
- быстрое обнаружение проблем безопасности;
- быстрое устранение неполадок в работоспособности и доступности сервисов;

- необходимость специального обучения сотрудников по безопастности облачных систем;
- большие вложения в информационную безопастность.

Перечислим угрозы, характерные для распределенных облачных систем:

– атаки на программное обеспечение;

– атаки на серверы облака;

– атаки на пользователя;

– атаки аутентификации;

– сетевые атаки;

– передача атак по цепи;

– DDoS атаки;

– атаки бокового канала – группа атака, направленная на слабые места в реализации криптосистемы.

Угрозы могут являться как внешними, так и внутренними.

Можно выделить следующие слабые места облачных систем:

1. Гипервизор, получение контроля над которым посторонним лицом позволяет получить полный доступ к ресурсам клиента;

Рисунок 1.3 – Структура системы с использованием облачных технологий

2. Сервер управления, атака на который приводит к нарушению или даже приостановке работы всей облачной инфраструктуры;

3. Виртуальная машина и приложения. Является самым уязвимый объект облачной системы. Это происходит потому, что клиенты облака взаимодействуют с приложениями на виртуальной машине на прямую.

4. Небезопасные интерфейсы и API. При использовании клиентами приложений, которые могут нанести вред облачной системе (умышленно или нет), при отсутствии инструментов анализа кода и приложений облачная система может пострадать от запуска этих вредоносных приложений.

Также к слабым местам облачной системы можно отнести уязвимость аутентификации пользователей, возможность перехват трафика или сервиса. Для устранения этих проблем необходимо применять современные криптографических алгоритмов разработанные для облачных систем [20].

На рисунке 1.4 представлена общая схема угроз для облачной системы.

Задача оптимизации системы информационной безопасности облачной системы необходимо определение эффективных механизмов защиты и их месторасположения для наибольшей эффективности всей системы безопасности в целом.

Таким образом, задачу оптимизации системы защиты распределенной облачной системы, можно описать следующими этапов.

1. Определяется архитектура распределенной облачной системы;

2. Определяются ограничения, которые будут наложены как всю систему в целом, так и отдельные её классы узлов;

3. Формируется список угроз, которые могут возникнуть для данной системы;

4. Формируются классы средств защиты для последующего выбора контрмер для распределения по узлам системы;

5. Формируются критерии оценки средств защиты в каждом конкретном классе;

6. Устанавливаются взаимосвязи между критериями оценки контрмер и значимости определенного критерия в противодействии угрозам;

7. Определяется эффективность, показываемая средствами защиты в зависимости от их расположения на различных типах узлов;

8. Формируется список механизмов обеспечения информационной безопасности (программных и аппаратных продуктов), представляющих классы контрмер;

9. Все контрмеры оцениваются исходя из заданных ранее ограничений для системы;

10. Расчет оптимального варианта размещения выбранных средств информационной защиты в рамках информации об архитектуре системы, используемых классах контр пер и введенных ограничениях для системы.

Рисунок 1.4 – Схема угроз облачной системы

Самым важным показателем системы информационной безопасности облака является показатель уменьшения ущерба системы, получающегося из суммы показателей ущерба для каждого компонента облачной системы.

Приведем все используемые виды средств защиты и возможные места их расположения. Они отображены в таблице 1.1.

Таблица 1.1 – Размещение средств защиты

Тип средств защиты	Цель	Точка размещения
Антивирусы	Антивирусная защита	Рабочие станции пользователей, серверы облачного провайдера
Брандмауэры	Постоянный контроль проходящего через систему трафика; Запрет подключения и обмена данными с узлами извне сети не имеющими на то разрешения	Рабочие станции пользователей, серверы облачного провайдера, коммутаторы, маршрутизаторы
Средства аутентификации и идентификации пользователей	Проверка подлинности пользователей и допуск к работе с системой только пользователей, прошедших проверку	Рабочие станции пользователей, серверы облачного провайдера, маршрутизаторы
Средства протоколирования и аудита	Запись всех действий пользователей, производимых в системе, и проверка несанкционированной деятельности пользователей	Рабочие станции пользователей, серверы облачного провайдера
Система обнаружения вторжений	Отслеживание и предотвращение попыток получить доступ к облачной системе и данным в ней посторонним лицами	Серверы облачного провайдера, маршрутизаторы, коммутаторы
Песочница, средства анализа кода	Анализ кода размещаемых на облаке приложений, не допуская установку и запуск вредоносных программных элементов в системе	Серверы приложений облачного провайдера
Антишпионы	Обнаружение различных шпионских программ и элементов программного обеспечения	Рабочие станции пользователей, серверы облачного провайдера
VPN	Создание защищенного канала для передачи данных внутри открытых каналов (например интернета)	Рабочие станции пользователей, серверы облачного провайдера, мобильные клиенты, маршрутизаторы
Система резервирования данных	Возможность восстановления приложений, данных и структуры системы после реализации каких-либо угроз	Серверы облачного провайдера

Приведем примеры различных средств защиты, которые можно использовать для обеспечения соответствующего уровня защиты облачной системы.

Антивирус: BitDefender, Avira, Kaspersky Internet Security, ESET NOD32.

Брандмауэр: Comodo Internet Security, Total AV Remote Firewall, Avira Internet Security, SpyShelter, Barracuda NG Firewall.

Средства идентификации и аутентификации(программное): JaCarta Management System, TeddyID Login, SafeNet Network Logon, Рутокен Логон.

Средства идентификации и аутентификации (Аппаратный ключ): eToken, Hardlock, HASP, IronKey, iButton, ruToken.

Средства контроля доступа: Криптон-Щит, Dallas Lock, Centrify Server Suite, Secret Net, Аккорд.

Средства протоколирования и аудита: КОМРАД, DATAPK, ePlat4m.

Система обнаружения вторжений: Industrial Security Incident Manager, Kaspersky Industrial CyberSecurity, Cisco IPS, TippingPoint, Sourcefire.

Песочница, средства анализа кода: BLUE COAT SYSTEMS Advanced Threat Protection, FireEye Malware Analysis (AX), Sandboxie.

Система резервирования данных: CommVault, Veeam Kasten K10, Acronis «Защита Данных».

VPN: Private Internet Access, TorGuard, ExpressVPN.

Инфраструктура открытых ключей: Entrust PKI, iPlanet CMS, КриптоАРМ.

Средства обеспечения целостности: HP Cluster Extension, Security Vision, Астерос.

Криптографические средства: Secret Disk Enterprise, InfoWatch CryptoStorage, Rohos Disk.

Приведем пример расстановки средств защиты в облачной системе: BitDefender, Comodo Internet Security, IronKey, TeddyID Login, CommVault, Sandboxie, Cisco IPS.

Такая расстановка средств информационной безопасности системы позволяет получить высокую надежность и безопасность облачной системы. Следует отметить, что вместо отобранных средств защиты могут использоваться эквивалентные средства защиты, но при этом может измениться эффективность защиты. Например, антивирус BitDefender можно заменить на Avira Internet se-

curity, обладающий той же функциональностью, но при этом показатели антивируса Avira по критерию «производительность» будут ниже, чем у Bitdefinger.

Равенство средств защиты отображается в том они могут быть взаимозаменяемыми средствами другого класса, если они имеют похожие функции.

1.4. Алгоритмы шифрования применяемые в распределенных облачных системах

В связи с тем, что применение облачных систем позволяет получать доступ к данным с различных устройств и в самых различных местах возникает необходимость как разграничения доступа к информации, так и шифрование хранимой информации. Так как доступ к облаку осуществляется разными людьми с различными правами доступа, то стандартные алгоритмы шифрования теряют свою актуальность. Поэтому с развитием и распространением облачных систем начали развиваться и связанные с ними алгоритмы шифрования, усиливающие защиту информации. Такими алгоритмами стали алгоритмы, использующие для расшифровки присвоенные пользователю атрибуты. Приведем подобный алгоритм.

1.4.1. PP-CP-ABE -шифрование

PP-CP-ABE - шифрование построено с использованием билинейного соединения, а также тайной схемы разделения, которые кратко представлены ниже.

1) Билинейное соединение: Соединение - билинейной функции $e: G_0 * G_0 \to G_1$ где $.G_0.$ и $.G_1.$ две мультипликативных циклических группы с большим главным порядком p.

Эти соединения обладают следующими свойствами:

Билинейность $e\left(P^a, Q^b\right) = e\left(P, Q\right)^{ab}$, $\forall P, Q \in G_0, \forall a, b \in Z_p^*$

Невырожденность: $e\left(g, g\right) \neq 1$ где g является генератором G_0.

Вычислимость: имеется эффективный алгоритм вычисления соединения.

2) Секретный Обмен: (t,n) секретный обмен, применяется для разложения информации на части n и любые части t могут воссоздать информацию, данные не будут раскрыты если их соединение не превысит t.

1.4.2. Настройка системы и ключа

Доверенный источник первой установки PP-CP-ABE системы выбирает билинейной оператор: $e: G_0 * G_0 \to G_1$ простого порядка δ_p генератора g. Также он выбирает два случайных параметра α, $\beta \in Z_p$. Открытые параметры публикуются в виде:

$$PK = G_0, g, h = g^{\beta}, f = g^{\frac{1}{\beta}}, e(g,g)^{a}.$$

Главный ключ $ГК = (\beta, g^{\alpha})$, известен только источнику первой установки системы.

Каждый клиент, имеющий доступ к зашифрованной информации обладает закрытым ключом в базе программного или аппаратного источника идентификации, аутентификацию и авторизацию. В качестве атрибута шифрования может выступать любая строка, уникально определяющая пользователя и уровень доступа. Алгоритм генерации уникальных ключей использует в качестве входных данных набор атрибутов S, назначенные пользователю, и выводит набор секретного ключа компоненты соответствующие каждому из атрибутов S.

Алгоритм генерации ключа:

1) Выбираем случайно $r \in Z_p$

2) Случайным образом определяем коэффициент $r_j \in Z_p$ для каждого параметра $j \in S$.

3) Генерируем закрытый ключ:

$$SK = \left\langle D = g^{\frac{\alpha+r}{\beta}}; \forall j \in S: D_j = g^{r} \times H(j)^{r_j}; D'_j = g^{r_j} \right\rangle$$

4) Посылаем закрытый ключ SK к доверенному источнику DO используя защищенный канал передачи данных.

1.4.3. Аутсорсинговое PP-CP-ABE шифрование

Для стороннего расчета шифрования и сохранения конфиденциальности данных, доверенному источнику требуется задать дерево доступа $T = T_{ESP} \wedge T_{DO}$, объединяющей два поддерева: дерево политики доступа пользователей T_{ESP} и управляющее дерево доступа к информации T_{DO}.. На рисунке 1.5 приведен пример дерева доступа T

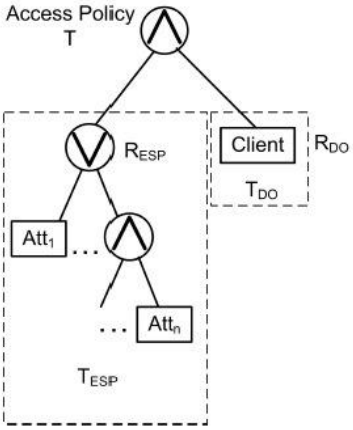

Рисунок 1.5 – Дерево доступа T

Чаще всего, на практике, дерево управляющего доступа T_{DO} обладает только одним параметром, которые можно определить в виде многочлена 1-го порядка $q_R(x)$ и наборов $s = q_R(0)$, $s_1 = q_R(1)$ и $s_2 = q_R(2)$ $s=q_R(0)$, $s_1=q_R(1)$. После этого доверенный источник DO отправляет данные $\{s_1, T_{ESP}\}$ ESP которые отмечаются следующим образом:

$$DO\overrightarrow{\{s_1, T_{ESP}\}}ESP$$

ESP запускает следующий алгоритм шифрования:

1. $\forall x \in T_{ESP}$ случайным образом выбранный многочлен q_x со степенью $d_x = k_x - 1$, где k_x – секретное пороговое значение совместного использования:

а. Для корневого узла T_{ESP} то есть R_{ESP}, выбирает $d_{R_{ESP}}$ - степень многочлена с $q_{R_{ESP}}(0) = s_1$

б. $\forall x \in T_{ESP} / R_{ESP}$ наборы d_x – степень многочлена с $q_x(0) = q_{parent(x)}\left(index(x)\right)$

2. Формирует временный зашифрованный текст

$$CT_{ESP} = \left\{ \forall_y \in Y_{ESP} : C_y = g^{q_y(0)}, C_y' = H\left(att(y)\right)^{q_y(0)} \right\},$$

где Y_{ESP} множество конечных узлов в T_{ESP}.

В то же время, DO выполняет следующие операции:

1. Выполняет Шифрование $\left(s_2, T_{DO}\right)$ и получает:

$$CT_{DO} = \left\{ \forall_y \in Y_2 : C_y = g^{q_y(0)}, C_y' = H\left(att(y)\right)^{q_y(0)} \right\}$$

2. Вычисляет $\hat{C} = Me(g,g)^{as}$ и $C = h^s$, где M это сообщение.

3. Посылает CT_{DO}, $\hat{C}$, C *в* ESP

$$DO \xrightarrow{\{CT_{DO}, \hat{C}, C\}} ESP$$

4. При получении сообщения от DO, ESP генерирует следующий зашифрованный текст:

$$CT = \left\langle T = T_{ESP} \wedge T_{DO}; \hat{C} = Me(g,g)^{\alpha s}; C = h^s; \forall_y \in Y_{ESP} \cup Y_{DO} : C_y = g^{q_y(0)}; C_y' = H\left(att(y)\right)^{q_y(0)} \right.$$

После выполнения процесса шифрования, исполнитель ESP пересылает заказчику зашифрованный текст CT.

1.4.4. Алгоритм дешифрования

Алгоритм дешифрования достаточно дорогостоящий в вычислительном отношении. Эта проблема возникает в следствии того, что применение билинейных соединений требуют больших вычислительных ресурсов. Алгоритм PP-CP-ABE позволяет передать этот процесс стороннему источнику (аутсорсинг). При этом на стороне аутсорсинга зашифрованные данные не подвергаются угрозе.

Для защиты данных DO использует закрытый ключ, выбрав случайным образом $t \in Z_p$ затем вычисляется $\tilde{D} = D^t = g^{t(a+r)/\beta}$. Обозначим закрытый ключ SK:

$$SK = \tilde{D} = g^{t(a+r)/\beta}, \forall j \in S : D_j = g^r \times H(j)^{r_j}, D_j' = g^{r_j}$$

Прежде, чем передать данные стороннему источнику DSP, доверенный источник DO проверяет, являются ли атрибуты доступа уникальными и описывают ли они каждого пользователя, имеющего соответствующий доступ. Если никаких проблем нет, то доверенный источник DO посылает закрытый ключ SK в DSP и просит его службу шифрования SSP прислать зашифрованный текст в DSP. Получив запрос SSP посылает $CT' = \left\{T; C = h^s; \forall y \in Y_1 \cup Y_2 : C_y = g^{q_y(0)}; C_y' = H\left(att(y)\right)^{q_y(0)}\right\}$ и $CT' \subset CT$ для DSP:

$$SSP \xrightarrow{\{CT'\}} DSP .$$

После того, как DSP получит SK и CT' затем происходит расшифровка $\left(SK, CT'\right)$ следующим образом:

1) $\forall y \in Y = Y_{ESP} \cup Y_{DO}$ DSP рекурсивно исполняет функцию расшифровки узла $\left(CT', SK, R\right)$, где R является корнем дерева доступа T. Функция рекурсии определена в работе [21]. Процесс расшифровка узла $\left(CT', SK, y\right)$ и алгоритм расшифровки выглядит следующим образом:

$$DecryptNode\left(CT', SK, y\right) = \frac{e\left(D_i, C_y\right)}{e\left(D_i', C_y'\right)} = \frac{e\left(g^r \times H(i)^{r_i}, g^{q_y(0)}\right)}{e\left(g^{r_i}, H(i)^{q_y(0)}\right)} = e(g,g)^{rq_y(0)} = F_y \qquad (1.1)$$

Обработка рекурсии происходит в следующей порядке: для $\forall y$ дочерний элемент x вызывает функцию (1.1) и сохраняет в файл как Fy. Пусть Sx является произвольным параметром, k_x - размер дочерних узлов y, DSP вычисляет:

$$F_x = \prod_{y \in S_x} F_y^{\Delta_i, S_x'(0)} = \prod_{y \in S_x} \left(e(g,g)^{r * q_y(0)}\right)^{\Delta_i, S_x'(0)} = \prod_{y \in S_x} \left(e(g,g)^{r * q_{parent(y)(index(y))}}\right)^{\Delta_i, S_x'(0)} =$$

$$= \prod_{y \in S_x} \left(e(g,g)\right)^{r * qx(i) * \Delta_i, S_x'(0)} = e(g,g)^{rq_x(0)}$$

где $i = index(z)$ и $S_x^{'} = \{index(z) : z \in S_x\}$

В конце, рекурсивный алгоритм возвращает $A = e(g,g)^{rs}$

2) Затем высчитывается

$$e(C, \tilde{D}) = e\left(h^s, g^{t(a+r)/\beta}\right) = e(g,g)^{trs} * e(g,g)^{tas}$$

3) Посылается $\left\{A = e(g,g)^{rs}, B = e(C, \tilde{D}) = e(g,g)^{trs} * e(g,g)^{tas}\right\}$ в DO

$$DSP \overset{\{A,B\}}{\rightarrow} DO$$

При получении $\{A, B\}$, DO вычисляет $B' = B^{1/t} = e(g,g)^{rs} * e(g,g)^{as}$, а затем восстанавливает сообщение:

$$M = \frac{\tilde{C}}{(B' / A)} = \frac{Me(g,g)^{as}}{\left(e(g,g)^{rs} * e(g,g)^{as}\right) / e(g,g)^{rs}}.$$

Таким образом и происходит расшифровка текста.

2. МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОБЛАЧНОЙ СИСТЕМЫ

2.1. Построение модели угроз информационной безопасности для распределенной облачной системы

Сейчас для любой компании обеспечения сохранности своей информации является первостепенной задачей. Так как все больше и больше различных кампаний и предприятий применяют в своей работе распределенные облачные системы, то возникает необходимость в реализации современной системы защиты информации на облачных системах. Однако, процесс построения системы информационной безопасности не заканчивается процессом проектирования системы, а должен являться непрерывным поискам угроз, средств защиты и модификации механизмов безопасности.

Угрозы – совокупность условий и факторов, создающих возможность получения злоумышленником несанкционированного доступа в систему, и взаимодействия с данными, хранящимися в системе [22].

Существует множество классификаций угроз информационной безопасности. Основные классификации и угрозы, относящиеся к соответствующему классу представлены на рисунке 2.1.

При создании системы защиты данных необходимо уделять большое внимание вопросу об оценке возможных угроз информационной безопасности. Имеется несколько способов решения этой проблемы. Чаще всего эта задача решается через нахождение вероятностей и возможного ущерба от их реализации. К примеру, в работе [23] использован следующий подход: для каждой возможно угрозы задается уровень влияния *Infact* этой угрозы на состояние информации (конфиденциальность, целостность, доступность). Так как каждая угроза реализуется в системе не со 100% шансом, то для каждой угрозы существует своя вероятность реализации *Exploitability* .

Именно этими параметрами и определяется базовый уровень угрозы BS. В работе [23] предложена следующая формула для оценки базового уровня угрозы:

$$BS = \left(\left(0.6 \cdot Impact \right) + \left(0.4 \cdot Exploitability \right) - 1.5 \cdot f\left(Impact \right) \right).$$

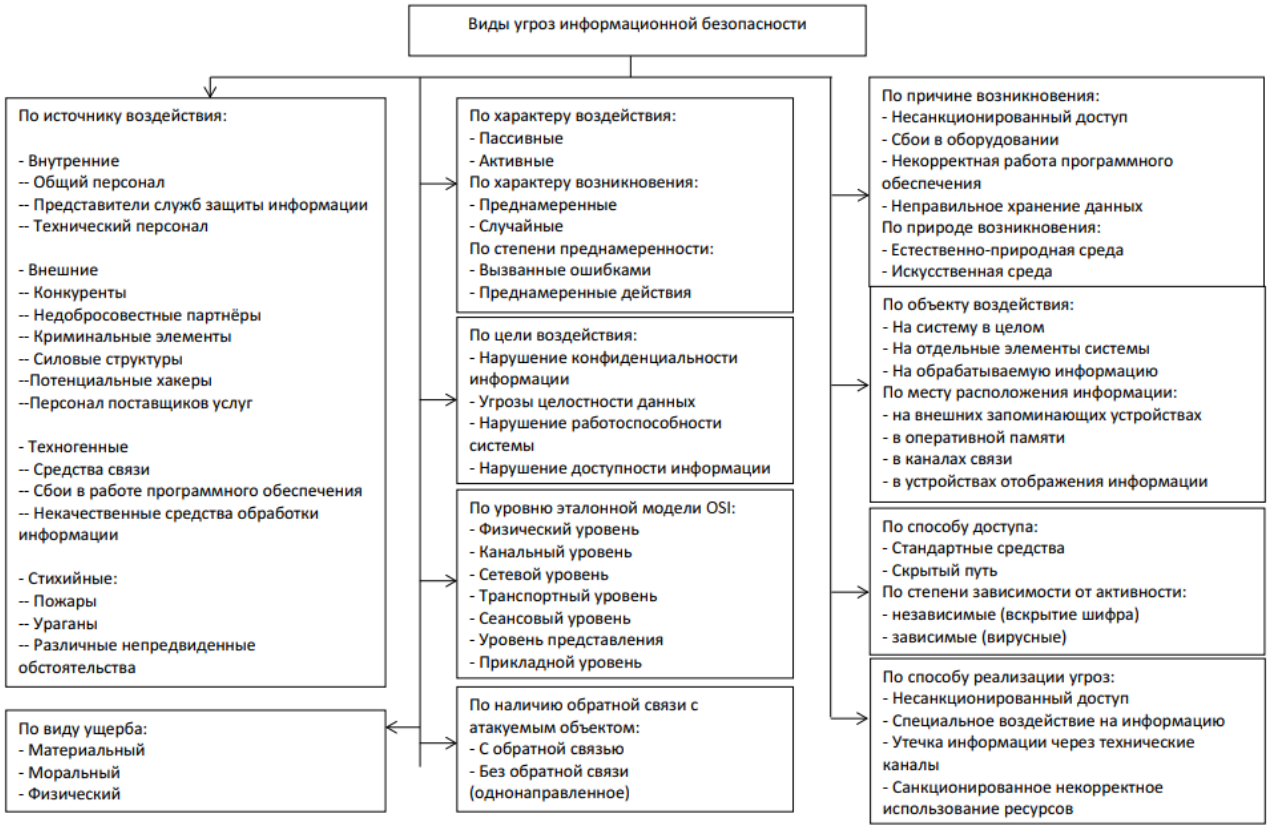

Рисунок 2.1 – Различные классы угроз информационной безопасности

В работе [24] получены следующие формулы для вычисления параметров $Impact$ и $Exploitability$.

Для расчета уровня влияния угрозы $Impact$ можно использовать формулу:

$$Impact = 10.41 \cdot \left(1 - \left(1 - ConfImpact \right) \cdot \left(1 - IntegImpact \right) \cdot \left(1 - AvailImpact \right) \right)$$

Формулой

$$Exploitability = 20 \cdot AccessVector \cdot AccessComplexity \cdot Authentication$$

можно рассчитать вероятность реализации угрозы.

Однако, такая методика оценки угроз не является комплексной. Более совершенный алгоритм оценки угроз дан в работе [25]. Для оценки угроз используется не два параметра, а гораздо большее количество. Формулу, описывающую процесс оценки угроз, можно записать следующим образом:

$$R = P_{угр} R_n C \frac{K_0 + K_t}{2} \cdot 100\%,$$

где R является численным показателем, отражающим шанс реализации угрозы, $P_{угр}$ – вероятность того, что по крайнее мере хотя бы одна угроза, принадлежащая множеству актуальных угроз, будет реализована в системе, R_n – вероятность, того что система безопасности не выполнят требования соответствующего государственного стандарта, C – ценность актива, K_0 – шанс, того что при угроза возникнет из-за использования организационных уязвимостей, K_t – вероятность использования злоумышленником технических уязвимостей системы.

Применение комплексного подхода к оценке угроз информационной безопасности системы дается в работе [26]. Для этого каждой угрозе присваивается несколько параметров: «Ущерб из-за реализации угрозы в совокупности» $Price_j$, «Приоритет угрозы» $Select_j$, «Вероятность возникновения и реализации угрозы» $Opportunity_k$. Тогда, используя угрозы, описанные подобным набором параметров, получим следующую модель угрозы t, которая является вектором нечетких характеристик $f_{pT}(t)$:

$$f_{pT}(t) = \left(Price_j, Select_j, Opportunity_k \right).$$

Стоит брать во внимание то, что эти подходы лучше всего подходят для относительно небольших систем, где оценка угроз информационной безопасности необходима лишь для поиска самых незащищенных мест системы. Для того чтобы провести реконструкцию в структуре системы, на основе этих данных, необходимо наличие более детального подхода.

Помимо описанных методов оценки угроз также применяются метод экспертных оценок [27], применение модели «хищник-жертва» для моделирования

атак на систему и оценки эффективности защиты [28], [29] и некоторые другие методы.

Все эти методы оценивают только угрозы, не обращая внимания на механизмы защиты и их взаимосвязь. Поэтому комплексный подход, учитывающий угрозы, механизмы защиты, их эффективность и взаимосвязь является перспективным направление исследования информационной безопасности облачных систем.

Построим математическую модель угроз.

Пусть множество угроз D представляет собой совокупности кортежей данных:

$$D_j = \left\langle K_i, P_{ij}, DMG_{i,j} \right\rangle,\ j = 1,...,DCOUNT, \tag{2.1}$$

в котором параметр $DCOUNT$ – количество угроз распределенной облачной системе, K_i, $1 = 1,...,KCOUNT$ – объекты на которые воздействуют угрозы, P_{ij}, $j = 1,...,DCOUNT$, $i = 1,...,KCOUNT$ – вероятность того, что угроза D_j будет реализована на объекте K_i, DMG_{ij}, $j = 1,...,DCOUNT$, $i = 1,...,KCOUNT$ – ущерб, который получит объект K_i если угроза D_j будет реализована на этом объекте.

Такое рассмотрение модели угроз позволяет изучить работу механизма защиты облачной системы как взаимодействия аппаратных узлов системы и её программных частей.

Использования подобной модели угроз требует наличие способа оценки вероятности возникновения угроз и потенциальных ущербов реализации каждой угрозы.

Для этого построим следующий алгоритм оценивания угроз, состоящий из двух основных этапов.

1) определение самых главных факторов, оказывающих влияние на шанс возникновения угрозы на узлах конкретного типа. Можно выделить следующие факторы:

а) возникновение угрозы в следствии отрасли работы компании или

предприятия, обеспечивающего информационную защиту;

б) возникновение угрозы на конкретном типе узлов;

в) возникновение угрозы в стране, где территориально расположен исследуемый узел.

Тогда вероятность P_{ij} того, что угроза D_j будет реализована на объекте K_i можно задать следующей формулой вероятности появления трёх независимых совместных событий

$$P_{i,j} = P_{ij}^{otr} + P_{ij}^{node} + P_{ij}^{area} - P_{ij}^{otr} \cdot P_{ij}^{node} - P_{ij}^{node} \cdot P_{ij}^{area} - P_{ij}^{otr} \cdot P_{ij}^{area} + P_{ij}^{otr} \cdot P_{ij}^{node} \cdot P_{ij}^{area}.$$

В этом выражении P_{ij}^{otr} является вероятность того, что угроза D_j появится в отрасли деятельности предприятия, P_{ij}^{node} – вероятность того, что угроза D_j появится в типе узлов, к которому относится узел K_i, P_{ij}^{area} – вероятность того, что угроза D_j появится в стране, к торой находится физическое расположение узла K_i.

2) вычисление потенциального ущерба DMG_{ij}, причиненного узлу K_i в следствии, того, что угроза D_j была реализована на этом узле. Этот потенциальный ущерб можно определить как сумму ущерба от получения злоумышленниками доступа к данным DMG_{ij}^{data} на узле K_i в следствии реализации угрозы D_j, ущерба аппаратного или программного обеспечения DMG_{ij}^{tech} узла K_i и ущерба от простоя оборудования DMG_{ij}^{losses}, за время устранения угрозы и восстановления узла K_i:

$$DMG_{ij} = DMG_{ij}^{data} + DMG_{ij}^{tech} + DMG_{ij}^{losses}.$$

Измерение всех показателей будем производить в условных единицах.

Такая методика оценки угроз и потенциального ущерба позволяет использовать для оценки параметров угроз и ущерба данные из открытых источников информации, что обеспечивает высокую точность определения количественных показателей в модели угроз (2.1).

2.2. Элементы оптимальной модели облачной системы

Построим модель архитектуры информационной безопасности распределенной облачной системы для оптимизации механизмов защиты и мест их установки. Такая модель может быть представлена несколькими компонентами:

1. Множество угроз *D*, которое было описано выше в разделе 2.1;

2. Общие условия реализации системы (ограничения системы) $UL_j,\ j=1,...,ULCOUNT$, где $ULCOUNT$ – количество таких ограничений. Общими ограничениями являются ограничения накладываемы на всю облачную систему в целом, например главным из общих ограничений является объем денежных средств UL_1, которые организация готова потратить на построение системы информационной безопасности;

3. Локальные условия реализации системы $LL_j,\ j=1,...,LLCOUNT$ где $LLCOUNT$ – количество таких ограничений. Локальными ограничениями являются ограничения накладываемые на конкретные узлы системы. Примерами локальных ограничений может выступать например:

Частота процессора LLK_{11} на классе узлов K_1;

Объём оперативной памяти LLK_{21} на классе узлов K_1;

Объём внутренней памяти LLK_{31} на классе узлов K_1;

4. Совокупность всех элементов распределенной облачной системы

$$K=\{K_i\}=\langle LLK_{ik},\ CNT_i,\ KPR_i\rangle,\ i=1,...,KCOUNT$$

где $KCOUNT$ – количество элементов распределённой системы, CNT_i – количество узлов типа K_i, KPR_i – номер родительского узла в архитектуре облачной системы.

Так как для облачной системы установка локального сервера не является необходимой, то можно выделить следующие типы узлов, входящие в распределенную облачную систему:

а) $KS=\{KS_j, j=1,...CNT_{KS}\}$ – множество облачных серверов, хранящих программные механизмы системы информационной безопасности;

б) $KL = \left\{ KL_j, j = 1,...CNT_{KL} \right\}$ – множество локальных узлов, являющихся рабочими станциями используемыми пользователями;

в) $KN = \left\{ KN_j, j = 1,...CNT_{KN} \right\}$ – множество узлов, включающее в себя сетевое оборудование и аппаратные средства защиты информации;

5. Множество классов средств защиты информации $N = \left\{ N_m = \left\langle C_{ml},\ o_{mz} \right.\right.$

$\left.\left. O_{mz}, O_{mz}^{\lim},\ O_{mz}^{sign},\ EKN_{mi},\ IND_m, IND_{mzj},\ PRDC_{mzj},\ DRDC_{mzj} \right\rangle,\ m = 1,...,NCOUNT \right\}$, где

$C_{ml},\ l = 1,...,CCOUTT_m,\ m = 1,...,NCOUNT$ – средства защиты входящие в данный класс;

$O_{mz},\ z = 1,...,OCOUTT_m,\ m = 1,...,NCOUNT$ – критерии по которым сравнивается разные элементы данного класса средств защиты;

$O_{mz}^{\lim},\ z = 1,...,OCOUTT_m,\ m = 1,...,NCOUNT$ – идеальное значение средства защиты данных по критерию O_{mz};

$O_{mz}^{sign} = \left\{ -1,1 \right\},\ z = 1,...,OCOUTT_m,\ m = 1,...,NCOUNT$ – характеристика критерия O_{mz}, показывающая стремится ли значения критерия O_{mz} к своему минимальному или максимальному значению;

$EKN_{mi},\ i = 1,...,KCOUTT_m,\ m = 1,...,NCOUNT$ – показатель эффективности установки средства класса N_m относительно узла сети K_i;

ND_m - показатель равный 1, в случае если средства данного класса уменьшают вероятность реализации угрозы и -1 если снижают потенциальный ущерб;

$IND_{mzj} = \left[0,1 \right]$ – показывает уровень влияния критерия O_{mz} на противодействие угрозе D_j;

$PRDC_{mzj}$ – максимальное сокращение вероятности того, что угрозы D_j будут реализованы в системе, при условии, что критерий $O_{mz} = O_{mz}^{\lim}$;

$DRDC_{mzj}$ – максимальное сокращение потенциального ущерба, который

может возникнуть если угрозы D_j будут реализованы в системе, при условии, что критерий $O_{mz} = O_{mz}^{\lim}$;

6. Механизмы защиты информации $C_{ml} = \langle OC_{mlz}, LLC_{mli}, ULC_{mli}, KS_{ml}, IUL_{mi} \rangle$, $l = 1,...,CCOUNT_m$ где

$CCOUNT_m$ – количество используемых средств информационной безопасности для защиты по противодействию угрозам класса N_m;

OC_{mlz} – показатель данного механизма информационной защиты по критерию оценки эффективности средства O_{mz} внутри соответствующего класса;

LLC_{mli} – эффективность расхода ресурса LL_i;

ULC_{mlj} – эффективность расхода общего ресурса UL_i;

$KS_{ml} = [-1,1]$ – показывает влияние на эффективность данного средства защиты при наличии эквивалентного средства информационной защиты на узле вышестоящего уровня;

$IUL_{mi} = \{-1,1\}$ – показывает наличие или отсутствие расхода общего ресурса ULC_{mli} как для всей системы, так и для элементов, на которых размещен данный механизм защиты C_{ml};

Более подробно распишем различные механизмы для противодействия угрозам облачной системе и критерии их оценки:

а) $NB = \{NB_l, l = 1,...,CCOUNT_{NB}\}$ – брандмауэры.

Брандмауэры можно оценить по следующим параметрам:

O_1^{NB} – предотвращение доступа к системе посторонними лицами;

O_2^{NB} – защита от внутренних атак;

O_3^{NB} – защита от прерывания процессов внутри облачной системы;

O_4^{NB} – создание журнала активности работы пользователей и приложений, подтверждение пакетами данных заданных условий, контроль прикладного протокола.

б) $NA = \{NA_l, l = 1,..., CCOUNT_{NA}\}$ – антивирусы

O_1^{NA} – защита от вирусов-червей;

O_2^{NA} – защита от вирусов-троянов;

O_3^{NA} – защита от вирусов-зомби;

O_4^{NA} . – защита от программ-блокировщиков;

O_5^{NA} – защита от программ-шпионов;

O_6^{NA} – блокирование неизвестного и известного вредоносного ПО, не принадлежащего к приведенным выше категориям;

O_7^{NA} –ложные срабатывания;

O_8^{NA} – система самозащиты антивируса.

в) $NF = \{NF_l, l = 1,..., CCOUNT_{NF}\}$ – механизмы аутентификации, идентификации и авторизации пользователей

O_1^{NF} – вероятность того, что в систему проникнет посторонний пользователь;

O_2^{NF} – вероятность того, что будет произведена ошибочная блокировка легитимного пользователя;

O_3^{NF} – удобство и простота установки, настройки и использования;

O_4^{NF} – возможность биометрической аутентификации и авторизации.

г) $NP = \{NP_l, l = 1,..., CCOUNT_{NP}\}$ – средства разграничения доступа.

O_1^{NP} – эффективность разграничения доступа пользователей с разным уровнем доступа к данным;

O_2^{NP} – защита загрузки операционной системы;

O_3^{NP} – физическая защита ЭВМ от вскрытия.

д) $NVL = \{NVL_l, l = 1,..., CCOUNT_{NVL}\}$ – средства по организации виртуальной локальной сети.

O_1^{NVL} – возможность переноса устройств;

O_2^{NVL} – возможность подключения нескольких виртуальных локальных сетей к одному и тому же порту;

O_3^{NVL} – возможность подключения одного устройства к нескольким виртуальным локальным сетям.

е) $NVP = \{NVP_l, l = 1,..., CCOUNT_{NVP}\}$ – VPN

O_1^{NVP} – возможность туннелирования и шифрования;

O_2^{NVP} – поддержка протокола PPTP;

O_3^{NVP} – поддержка протокола L2TP;

O_4^{NVP} – поддержка протокола IPSec;

O_5^{NVP} – поддержка протокола SSL.

ё) $NI = \{NI_l, l = 1,..., CCOUNT_{NI}\}$ – система обнаружения вторжений.

O_1^{NI} – определяет возможное количество обнаруженных одновременно вторжений;

O_2^{NI} – максимальное количество одновременных подключений к облачной системе;

O_3^{NI} – пропускная способность.

ж) $NPK = \{NPK_l, l = 1,..., CCOUNT_{NPK}\}$ – инфраструктура открытых ключей.

O_1^{NPK} – наличие собственной системы выдачи и проверки сертификатов;

O_2^{NPK} – возможность интеграции в системы баз данных.

з) $NW = \{NW_l, l = 1,..., CCOUNT_{NW}\}$ – средства обеспечения целостности данных.

O_1^{NW} – обеспечение целостности программных средств и обрабатываемой информации;

O_2^{NW} – проверка по контрольным суммам компонент программных

средств;

O_3^{NW} – возможность проверки целостности данных по хэш-функции.

и) $NC = \{NC_l, l = 1,..., CCOUNT_{NC}\}$ – криптографические средства.

O_1^{NC} – реализация различных криптографических алгоритмов;

O_2^{NC} – наличие реализации протокола SSL/TLS.

2.3. Проблема оптимизации структуры информационной безопасности для облачных систем

Одной из важных особенностей распределенных облачных систем является отсутствие общей архитектуры системы с явными связями между элементами такой системы. Рисунок 2.2 иллюстрирует эту особенность. Облачная система соединяется с интернетом лишь через облачные сервера и хранилища. И только к этим элементам происходит подключение локальных сетей и мобильных клиентов облачной системы.

Поэтому при создании системы информационной безопасности необходимо учитывать ряд дополнительных особенностей:

1. Так как облачная система состоит из множества элементов разных классов то различные угрозы воздействуют на разные элементы системы, а не на все облако. Т.е. при реализации угрозы j на узле i облачной системе будет нанесен ущерб DMG_0 с вероятностью P_{ij}. Из-за этого необходимо устанавливать целую систему из средств информационной безопасности для того, чтобы возможный ущерб все системе PDU стремился к минимальному своему значению, т.е. был минимален на каждом узле облака;

2. Различные механизмы противодействия угрозам могут показать совершенно различную эффективность своей работы при установке их в разных узлах облачной системы;

3. Некоторые механизмы защиты могут быть расположены только на конкретных узлах сети. Поэтому для оценки эффективности различных средств защиты информации введем коэффициент EKN_{im}, который отражает эффектив-

ность эффективность работы средства информационной безопасности из класса m на узлах типа i;

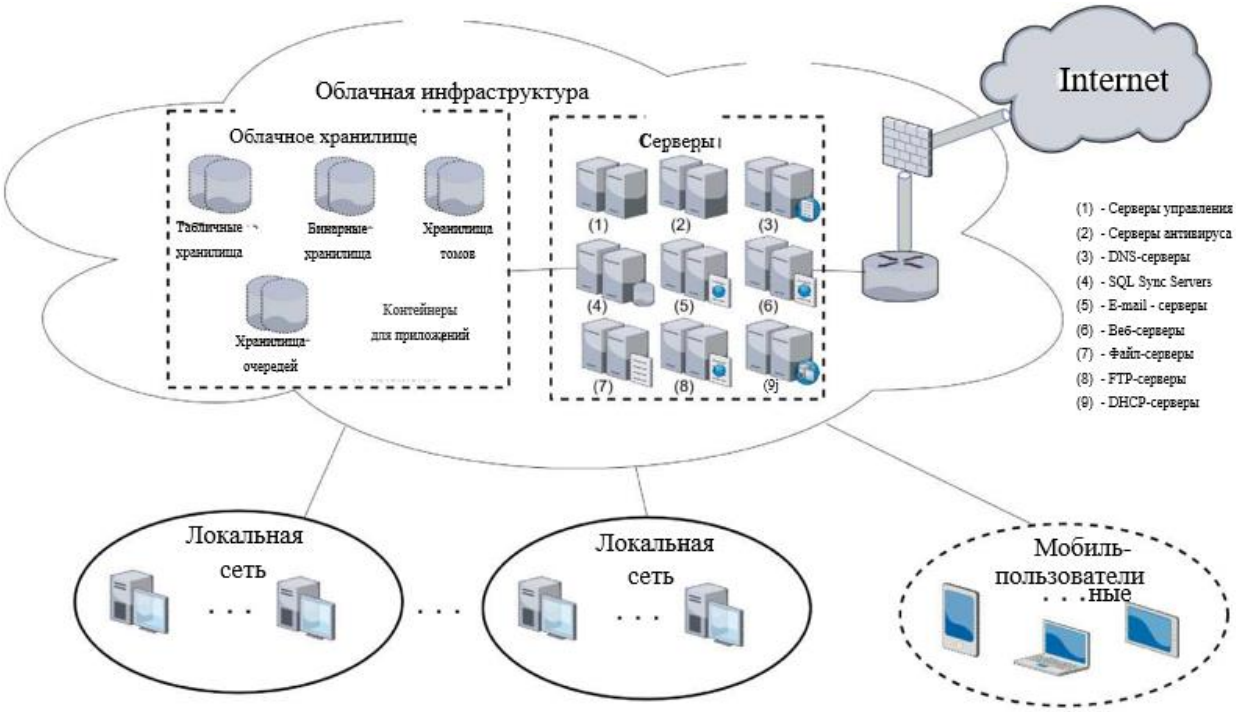

Рисунок 2.2 – Архитектура системы с использованием облачных вычислений

4. Существую эквивалентные механизмы защиты, которые могут принадлежать разным классам средств защиты. Они способны противостоять угрозам одного и того же типа несмотря на то, что принадлежат к разным классам защиты и имеют различные основные направления работы. Поэтому необходимо учитывать связь между различными механизмами противодействия угрозам и возможность замены на эквивалентные контрмеры;

5. Существуют средства защиты, которые показывают максимальную эффективность если в системе применяется как минимальное количество дублей, так и большое количество дублей данного механизма защиты, распределенного по множеству узлов. Поэтому для учета подобной ситуации добавим в модель коэффициент связности KS_{ml}, который будет показывать количественную эффективность данного средства защиты l из класса m.

Одновременно с параметрами модели, выраженными достаточно явно, существуют показатели, для которых определения точного значения невозмож-

но. Поэтому необходимо применять иные методы их оценивания. Приведем подходящую методику оценивания таких параметров:

1. В качестве приоритетной характеристики механизма защиты выберем его эффективность внутри своего класса. Для оценки эффективности необходимо провести эксперимент по противодействию различным угрозам, противодействию которым посвящен класс исследуемого механизма защиты. Для контрмеры l из класса противодействия угрозам m по критерию O_{mz} получим:

$$E_{mlz} = \frac{OC_{mlz}}{O_{mz}^{\lim}},$$

где

OC_{mlz} – полученный в ходе эксперимента показатель исследуемого средства защиты;

$O_{mz}^{\lim}$ – идеальное значение в эксперименте.

2. По мимо количественной оценки показателей эффективности контрмер, для некоторых из них лучше ввести экспертную оценку, так как являются субъективными, и оценить их можно только приближенно. Приведём список таких показателей:

EKN_{mi}, $i = 1,...,KCOUNT$ – показатель который отражает эффективность механизмов информационной безопасности системы класса *m* исходя из места установки механизма K_i в облачной системе;

$IND_{mzj} = [0,1]$ – показатель который отражает уровень участия критерия O_{mz} для защиты от угрозы D_j;

$PRDC_{mzj}$ – предельное уменьшение вероятности реализации угрозы D_j при условии, что критерий O_{mz} максимален;

$DRDC_{mzj}$ – предельное уменьшение возможного ущерба от реализации угрозы D_j при условии, что критерий O_{mz} максимален;

2.4. Построение оптимальной по затратам и ущербу модели распределённой облачной системы

Главной задачей при проектировании информационной безопасности облачной системы самой важной задачей является сокращение до минимума ущерба от возможной реализации угроз при минимальных затратах на построение и обслуживание этой системы безопасности. В начале построим модель для оценки уровня ущерба системе и потребуем, чтобы это ущерб стремился к минимуму. Формально данную задачу можно рассмотреть, как минимизацию суммарного ущерба системе PDL [31], т.е. необходимо минимизировать сумму урона на каждом узле облачной системы.

Этот показатель можно найти по формуле:

$$PDL_i = CNT_i \cdot \left(\sum_{j=1}^{DCOUNT} P_{ij} \cdot DMG_{ij} \right). \qquad (2.2)$$

В формуле (2.2) вероятность P_{ij} того, что угроза D_j будет реализована на узле K_i определяется по следующей формуле:

$$P_{ij} = P_{ij}^0 - PRD_{ij}$$

в которой P_{ij}^0 – вероятность реализации угрозы D_j на узле K_i при отсутствии каких либо механизмов защиты от угроз типа D_j;

PRD_{ij} – изменение вероятности реализации угрозы D_j на узле K_i при установке на узел K_i механизм защиты C_l. Этот показатель можно определить используя следующее выражение:

$$PRD_{ij} = \sum_{m=1}^{OCOUNT_m} \sum_{z=1}^{OCOUNT_m} \sum_{j=1}^{OCOUNT} \left(IND_{mzj} \cdot PRDC_{mzj} \cdot \sum_{l=1}^{CCOUNT_m} E_{mlz} \cdot x_{mli} \right),$$

где

E_{mlz} – показатель эффективности исследуемой контрмеры при противодействию угрозе D_j на узле облачной системы K_i по критерию O_{mz}.

x_{mli} – показатель, который указывает присутствует ли контрмера C_l из

класса N_m на узле K_i;

Рассчитать возможный ущерб DMG_{ij} понесенный из-за реализации угрозы D_j можно по формуле:

$$DMG_{ij} = DMG_{ij}^0 - DRD_{ij}$$

где

DMG_{ij}^0 – ущерб реализации угрозы D_j на узле K_i при отсутствии каких либо механизмов защиты от угроз типа D_j;

DRD_{ij} – изменение ущерба в случае реализации угрозы D_j на узле K_i при установке на узел K_i механизм защиты C_l. Этот показатель можно вычислить по формуле:

$$DRD_{ij} = \sum_{m=1}^{OCOUNT_m} \sum_{z=1}^{OCOUNT_m} \sum_{j=1}^{OCOUNT} \left(IND_{mzj} \cdot DRDC_{mzj} \cdot \sum_{l=1}^{CCOUNT_m} E_{mlz} \cdot x_{mli} \right).$$

Просуммировав ущерб на каждом элементе облачной распределенной системе получим следующую целевую функцию ущерба:

$$PDU = \sum_{i=1}^{KCOUNT} CNT_i \cdot \left(\sum_{j=1}^{DCOUNT} \left(P_{ij}^0 - P_{ij}^0 \left(\sum_{m=1}^{NCOUNT_m} \sum_{z=1}^{OCOUNT_m} \sum_{j=1}^{DCOUNT} \left(KPR_i \cdot IND_{mzj} \cdot \right. \right. \right. \right.$$

$$\left. \left. \left. \left. PRDC_{mzj} \cdot \sum_{l=1}^{CCOUNT_m} E_{mlz} \cdot x_{mli} \cdot (1 + KS_{ml}) \right) \right) \cdot \left(DMG_{ij}^0 - \right. \right. \right.$$

$$\left. \left. \left. - \sum_{m=1}^{NCOUNT_m} \sum_{z=1}^{OCOUNT_m} \sum_{j=1}^{DCOUNT} \left(KPR_i \cdot IND_{mzj} \cdot DRDC_{mzj} \cdot \sum_{l=1}^{CCOUNT_m} E_{mlz} \cdot x_{mli} \cdot (1 + KS_{ml}) \right) \right) \right) \right) \right) \quad (2.3)$$

Так как для оптимальной системы информационной безопасности необходимо свести ущерб к минимуму, то устремим функцию (2.3) к минимуму.

Таки образом данная модель дает возможность исследовать каждый класс применяемых контрмер и определить оптимальное количество x_{mli} необходимых механизмов защиты l из класса m, размещаемого на узле i.

Однако, максимальная эффективность построенной системы безопасно-

сти возможна лишь при условии неограниченных финансовых, аппаратных и других условий, что в реальности невозможно [31]. Поэтому, по мимо минимизации ущерба необходимо учитывать и затраты на использование различных контрмер. Это условие можно описать, как использование минимально возможного расхода ресурсов по общим и локальным ограничениям для построения необходимого уровня системы информационной защиты. Получим следующие условия:

$$\forall z_1^{LLCOUNT} \sum_{i=1}^{KCOUNT} \sum_{m=1}^{NCOUNT} \sum_{l=1}^{CCOUNT} LLC_{mlz} \cdot x_{mli} \to \min;$$

$$\forall z_1^{LLCOUNT} \sum_{i=1}^{KCOUNT} \sum_{m=1}^{NCOUNT} \sum_{l=1}^{CCOUNT} ULC_{mlz} \cdot x_{mli} \to \min;$$

Если ограничения заданы строго, то тогда к целевой функции (2.3) добавляем краевые условия:

$$\forall z_1^{LLCOUNT}, i_1^{KCOUNT} \sum_{m=1}^{NCOUNT} \sum_{l=1}^{CCOUNT} LLC_{mlz} \cdot x_{mli} \le LLK_{iz},$$

$$\forall z_1^{LLCOUNT}, i_1^{KCOUNT} \sum_{m=1}^{NCOUNT} \sum_{l=1}^{CCOUNT} ULC_{mlz} \cdot x_{mli} \le UL_z. \qquad (2.4)$$

Таким образом получаем, что при решении задачи оптимизации информационной безопасности облачных систем возникает как минимум два критерия оценки эффективности системы безопасности, т.к. при в том случае, если компромисс между максимальной эффективностью и минимальной стоимостью не будет найден, то получим либо дешёвую, но почти не эффективную структуру, либо высокоэффективную, но дорогую структуру обладающую высокими требования в аппаратной части облачной системы, что может сильно отразиться на быстродействии облака.

Поэтому выделим эти два критерия следующим способом:

1. Ущерб, полученный при реализации возможных угроз, должен, стремится к минимуму.

$$wk_1 = PDU \to \min.$$

2. Затраты на систему должны быть максимально низкими.

$$wk_2 = \sum_{i=1}^{KCOUNT} \sum_{j=1}^{NCOUNT} \sum_{l=1}^{CCOUNT} LLC_{mlz} \to \min;$$

$$wk_3 = \sum_{i=1}^{KCOUNT} \sum_{j=1}^{NCOUNT} \sum_{l=1}^{CCOUNT} ULC_{mlz} \to \min;$$

Применим метод свёртывания векторного критерия, учитывающий относительную необходимость отдельных критериев оптимальности с помощью построения скалярной функции F, являющейся обобщённым критерием касательно векторного критерия $wk(x)$:

$$\min F\left(\overline{y}, \overline{wk}\left(\overline{x}\right)\right),$$

где

$y = \{y_1, y_2, ..., y_{KC}\}$ – весовые коэффициенты важности отдельных критериев,

$x = \{x_1, x_2, ..., x_{KC}\}$ – вектор решений, анализируемых с помощью многокритериальной оптимизации.

В качестве обобщённых критериев могут выступать следующие варианты расчёта функции F:

1. Аддитивный критерий оптимальности:

$$F\left(\overline{y}, \overline{wk}\left(\overline{x}\right)\right) = \sum_{i=1}^{KC} y_i wk_i\left(\overline{x}\right);$$

2. Мультипликативный критерий оптимальности:

$$. F\left(\overline{y}, \overline{wk}\left(\overline{x}\right)\right) = \prod_{i=1}^{KC} y_i wk_i\left(\overline{x}\right);.$$

3. Среднестепенной обобщённый критерий оптимальности:

$$F\left(\overline{y}, \overline{wk}\left(\overline{x}\right)\right) = \left[\frac{1}{KC}\sum_{i=1}^{KC} y_i wk_i^{wp}\left(\overline{x}\right)\right]^{1/wp};$$

В этом случае задачу расчета оптимального варианта размещения механизмов информационной безопасности облачной системы можно представить как:

$$F = \sum_{i=1}^{KC} y_i wk_i \to \min,$$

где $y_i \geq 0,\ \sum_{i=1}^{KC} y_i = 1,\ KC$ – общее количество критериев оптимизации формирования информационной защиты, i – порядковый номер критерия, y_i – значение весового коэффициента для критерия i, wk_i – значение критерия i.

Весовые коэффициенты определяются экспертом при создании информационной защиты на основе потребностей и имеющихся возможностей в данной распределённой системе.

Методика экспертного оценивания заключается в следующем: существует множество экспертов $E = \{E_1, ..., E_{ECOUNT}\}$, где $ECOUNT$ – количество экспертов. На основании выделенных критериев оптимизации формирования информационной защиты составляется матрица индивидуальных оценок экспертов по критериям:

Таблица 2.1 – Оценки экспертов по критериям

	Эксперты		
Критерии	E_1	E_2	E_{ECOUNT}
wk_1	$wk_{i,1\,1}$	$wk_{i,1\,2}$	$wk_{i,1\ ECOUNT}$
wk_2	$wk_{i,2\,1}$	$wk_{i,2\,2}$	$wk_{i,1\ ECOUNT}$
wk_3	$wk_{i,3\,1}$	$wk_{i,3\,2}$	$wk_{i,1\ ECOUNT}$

Каждый из экспертов даёт важности критерия wk_i личную оценку $wk_{i,f}$ так, чтобы сумма его личных оценок всех критериев была равна 1:

$$\sum_{i=1}^{KC} wk_{i,f} = 1.$$

Затем высчитывается весовой коэффициент значимости критерия как среднее арифметическое всех оценок экспертов:

$$wk_i = \frac{\sum_{f=1}^{ECOUNT} wk_{if}}{ECOUNT}.$$

Именно эта формула и используется для оценки каждого критерия.

3. ПРОГРАММНАЯ РЕАЛИЗАЦИЯ РАЗРАБОТАННЫХ МОДЕЛЕЙ И ИХ ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ ДЛЯ ПРОЕКТИРОВАНИЯ АРХИТЕКТУРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЛАЧНЫХ СИСТЕМ

3.1. Программная реализация инструментария для построения и исследования архитектуры информационной безопасности облачных систем

Программная реализация предложенных моделей и алгоритмов, реализующих задачу поиска оптимальной стратегии формирования информационной безопасности распределённых систем, выполнена на языке C++ в среде Microsoft Visual Studio 2015. Концепция программного обеспечения заключается в том, что на основе имеющихся архитектуры системы и совокупности классов и средств защиты информации производится выбор оптимального варианта размещения средств защиты информации. Программный продукт содержит в себе следующие модули: модуль ввода данных, с которыми программа будет осуществлять работу, модуль настроек параметров алгоритма и модуль расчета оптимальной архитектуры средств защиты. Главное окно программы представлено на рисунке 3.1.

Рассмотрим эти модули:

1) Модуль ввода данных

В рамках работы данного модуля пользователем осуществляется ввод имеющихся у него в распоряжении классов средств защиты - *defenders_classes*, их компонентов - *defenders.* Вводятся угрозы информационной безопасности - *Dangers*. Также вводятся классы точек, на которых будут размещаться средства защиты - *points_classes*. Помимо этого, пользователь вводит относящиеся к классам точек локальные (*local_limits*) и глобальные (*united_limits*) ограничения. Исходя из этого, средства защиты также имеют значения, в процессе с расчёта сравниваемые с ограничениями, заданными на точках: *defenders_limits_united* и *defenders_limits_local*.

Важнейшим элементом модуля ввода данных является указывание показателей эффективности конкретного средства защиты на возможной точке его размещения;

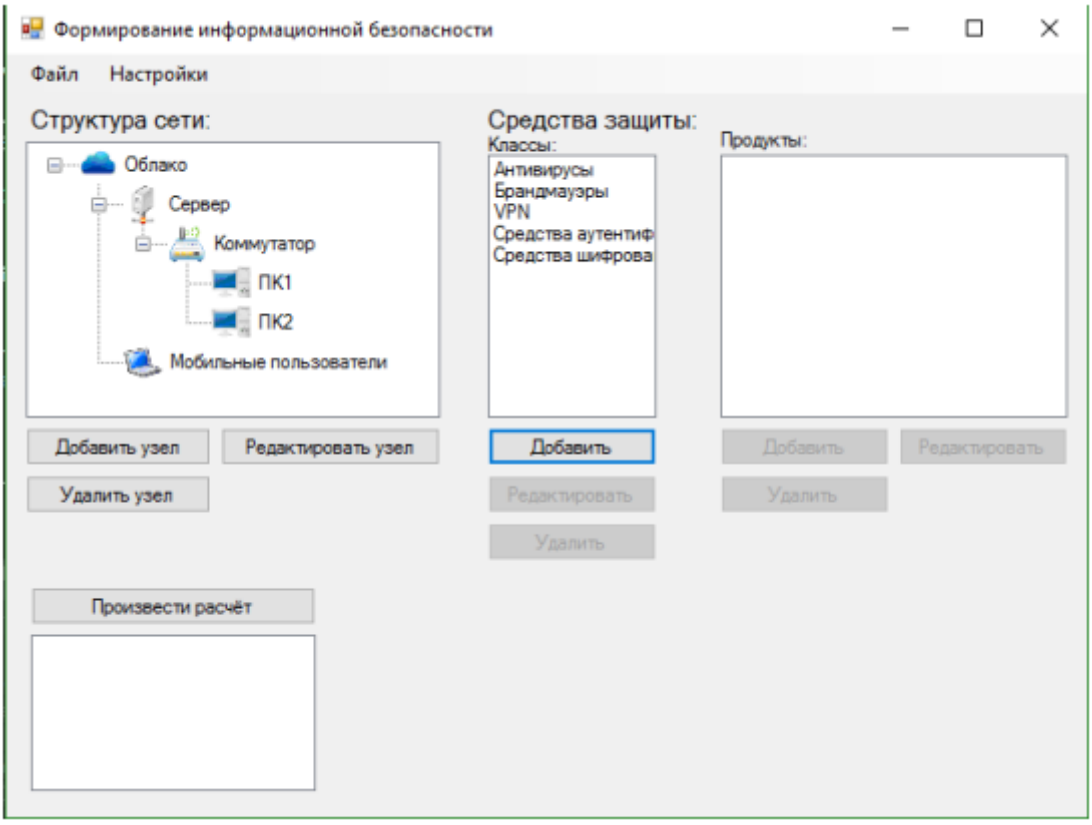

Рисунок 3.1 – Главное окно программы

2) Модуль настройки алгоритма. Данный компонент позволяет настроить параметры используемых при расчёте алгоритмов с целью их анализа и сравнения. Так, в настройках ГА можно выбрать тип стратегии отбора, мутации или кроссинговера;

3) Модуль расчёта. После ввода всех данных и настройки параметров расчёта начинает работу по вычислению эффективности различных наборов средств защиты информации.

Результатом работы программы является определение оптимального набора средств защиты информации и их расстановки таким образом, чтобы эффективность информационной безопасности была максимальной.

Программный продукт разрабатывался с использованием объектно-

ориентированного подхода, в результате чего можно выделить следующие классы, присутствующие в программе:

Класс *Main_Structure* объединяет все списки и методы, которые присутствуют в программной реализации математической модели выбора оптимального варианта размещения средств информационной защиты в распределённых системах. Он содержит следующие элементы:

4) список элементов класса *United_limits*, в котором хранятся наименования, значения и единицы измерения общих ограничений, накладываемых на систему.

5) список элементов класса *Local_limits*, в котором хранятся наименования и единицы измерения локальных ограничений, которые могут присутствовать в системе;

6) список элементов класса *DangersIS*, хранящий наименования всех угроз, которые могут угрожать распределённой системе;

7) список элементов класса *Points_of_network*, содержащий такие параметры типов узлов: наименование, количество узлов данного типа, индекс изображения, соответствующего классу, индекс родительского узла, если элемент не является корневым;

8) класс *ClassOfSecurity* заключает в себе наименование класса средств информационной безопасности, список критериев оценки средств защиты *Charachteristic* и матрицу связи характеристик с угрозами информационной безопасности.

3.2. Пример расчёта оптимального варианта размещения средств защиты в облачной системе

Для тестового расчета зададим экспериментальные данные, например описывающие некоторую небольшую компанию и средства защиты, используемые ею. Все данные задаются в соответствии с математической моделью, описанной в разделе 2.

Множество угроз D включает в себя следующие элементы:

D_1 – вирусная угроза;

D_2 – угроза внешней атаки;

D_3 – угроза атаки изнутри;

D_4 – возможность сбоя в подаче электропитания.

Общим ограничением, накладываемым на систему, является сумма денежных средств, которую руководство компании готово выделить на обеспечение информационной безопасности. Единица измерения - рубли:

$$UL_1 = 20000.$$

Бюджетные учреждения и предприятия малого бизнеса обычно имеют ограниченный бюджет для обеспечения информационной безопасности, вследствие чего при проектировании защиты стоит задача обеспечения приемлемого уровня безопасности при сравнительно малом объёме имеющихся средств и большом количестве имеющихся рабочих станций.

К локальным ограничениям, накладываемым на систему, приведенным в таблице 3.1, относится LL_1 – загрузка процессора.

Таблица 3.1 – Локальные ограничения, накладываемые на сеть

Локальное ограничение	Узлы сети				
	K_1	K_2	K_3	K_4	K_5
LL1	20	-	-	15	10

Структура сети подробно описана в таблице 3.2. Система имеет один головной сервер, один главный коммутатор, к которому подключены пять коммутаторов аудиторий. Кроме того, в системе присутствуют шесть серверов, выполняющие функции администрирования сети аудиторий, хранения данных специализированного программного обеспечения и др. Общее количество локальных рабочих станций равняется шестидесяти восьми.

Таблица 3.2. Описание узлов вычислительной сети

Обозначе-ние	Тип узла	Кол-во	Угрозы							
			D1		D2		D3		D4	
			P(0)	DMG (0)	P(0)	DMG (0)	P(0)	DMG (0)	P(0)	DMG (0)
K1	Сервер	1	0.8	10^4	0.6	10^4	0.1	10^4	0.4	10^4
K2	Коммутатор	1	0	0	0	0	0	0	0.4	500
Кз	Коммутаторы	5	0	0	0	0	0	0	0.4	200
K4	Серверы	6	0.5	10000	0.2	10000	0.1	10000	0.4	10000
K5	Локальные компьютеры	68	0.5	1000	0.4	1000	0.7	20000	0.4	1000

Далее определим множество N, описывающее классы средств защиты информации. Они представлены в таблице 3.3.

Таблица 3.3 – Классы средств защиты информации

Обозначение	Наименование	Крите-рии	Ед. изм.	Предель-ное значение	+/-	Уменьш. вероятности /ущерба	Влияние на угрозы			
							D1	D2	D3	D4
NA	Антивирусы	O_{11}	%	100	+	P	1	0	0.1	0
		O_{12}	%	100	+	P	0.5	0	0.2	0
NB	Брандмауэры	O_{21}	%	100	+	P	0.1	1	0.6	0
		O_{22}	%	100	+	P	0.1	0.7	1	0
NC	Системы ре-	O_{31}	%	100	+	P	0	0	0	1
		O_{32}	%	100	+	P	0	0	0	0.5

В качестве критериев выступают следующие показатели:

O_{11} – уровень защиты от вирусов;

O_{12} – уровень отсутствия ложных тревог;

O_{21} – уровень защиты от внешних атак;

O_{22} – уровень защиты от внутренних атак;

O_{31} – самозащита системы от взломов;

O_{32} – быстродействие системы.

После этого определим средства защиты, содержащиеся в каждом из

классов:

Таблица 3.4 – Средства защиты информации

Наименование	Класс	Значение по критериям		Значение по UL1	Комплексность параметра	Значение по LLi	Коэффициент связности
Avira	NA	O_{11}	87	15000	Да	5	0
		O_{12}	98				
Антивирус Касперского	NA	O_{11}	95	18000	Да	4	0
		O_{12}	95				
Bitdefender	NA	O_{11}	98	1800	Нет	5	0
		O_{12}	94				
		O_{32}	95				
Panda Security	NA	O_{11}	80	15000	Да	3	0
		O_{12}	88				
SpyShelter	NB	O_{21}	90	2300	Нет	4	-0.3
		O_{22}	82				
Comodo Security	NB	O_{21}	92	20000	Да	4	-0.3
		O_{22}	75				
CommVault	NC	O_{31}	95	2500	Нет	7	0
		O_{32}	83				
Actifio	NC	O_{31}	70	15000	Да	6	0

По итогам работы программы предложен следующий вариант размещения средств защиты на узлах сети:

K_1 - Avira, SpyShelter, CommVault;

K_4 - Avira;

K_5 - Avira.

Проведённое с помощью разработанной математической модели исследование показало, что использование предложенной программой структуры информационной безопасности на тестовом примере вычислительной сети позволяет снизить потенциальный ущерб информационной системе на 20680 рублей (при максимальном ущербе в 50000 и учете затрат средств на организацию информационной безопасности в размере 20000).

Можно выделить следующие особенности, с которыми сталкиваются предприятия последние годы:

1. Увеличение атак на облачные системы с помощью протокола удалённого доступа (23% атак) и почтовый спам (19% атак) [34];

2. Снижение опасности для банков в связи с возрастанием активности в сфере криптовалют (ущерб в данной области составил $168 млн.) [35];

3. Увеличение количества вирусов, специализирующихся на поражении Android-устройств, на 136% [36];

4. Возрастание количества программ-вымогателей, использующихся мошенниками, на 172 % [36].

С использованием данных сведений на разработанной модели оптимального размещения механизмов защиты проводился анализ типовых предприятий, использующих в своей работе облачные технологии. Проведённое исследование показало, что ущерб от таких атак может быть снижен в среднем на 100000000 рублей для крупных предприятий, ведущих свою деятельность на российском рынке.

ЗАКЛЮЧЕНИЕ

В ходе работы над дипломной работой были проанализированы основные угрозы и опасности для широкого внедрения облачных технологий в работу различных предприятий и учреждений. Была построена математическая модель информационной безопасности облачных систем. Для разработанной модели была реализована программа на языке C++ имитирующая облачную систему и различные угрозы этой системе. Разработанное программное обеспечение позволяет обеспечить информационную безопасность с учетом наиболее опасных угроз для конкретной компании. Это достигается за счет возможности построения уникальной архитектуры системы информационной безопасности и списка средств противодействия наиболее опасным и вероятным угрозам из различных классов угроз.

В качестве примера была продемонстрирована эффективность разработанного программного обеспечения в виде уровня потерь средств из-за проникновения в распределенную систему.

Проведён анализ безопасности типовых предприятий, использующих в своей работе облачные технологии. Проведённое на основании полученных из открытых отчётов сведений исследование показало, что ущерб от таких атак может быть снижен в среднем на 100 млн. рублей для крупных предприятий, ведущих свою деятельность на российском рынке. Результаты работы можно использовать специалистам в области информационной безопасности (системным аналитикам и администраторам, разработчикам облачных информационных систем) и математического моделирования (для проведения научных исследований в области защиты данных). Разработанные математические модели распределённых систем могут иметь дальнейшее развитие относительно учета конкретных характеристик и функций возможных средств вычислительной техники, программного обеспечения, технологий реализации различных концепций построения облака.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Гайдамакин, Н. А. Разграничение доступа к информации в компьютерных системах. / Н. А. Гайдамакин – Екатеринбург: Изд-во Уральского ун-та, 2003.– 328 с.

2. Скиба, В. Ю. Руководство по защите от внутренних угроз информационной безопасности / В. Ю. Скиба, В. А. Курбатов – СПб: Питер, 2008. – 322 с.

3. Богаченко, Н. Ф. Безопасность системы с ролевым разграничением доступа / Н. Ф. Богаченко // Решетневские чтения: сб. ст. XVI Междунар. науч. конф – Красноярск: Изд-во Сиб. гос. аэрокосмич. ун-т, 2012. – С. 654–655.

4. Гильмуллин, Т. М. Модели и комплекс программ процесса управления рисками информационной безопасности: Автореф. дис. канд. техн. наук: 05.13.18. – Казань, 2010. – 21 с.

5. Ширинкин, М. С. Модели и методы синтеза оптимальной иерархической структуры многоуровневого информационного комплекса промышленного предприятия: Автореф. дис. канд. техн. наук: 05.13.01. – Москва, 2011. – 21 с.

6. Голембиовская, О. М. Автоматизация выбора средств защиты персональных данных на основе анализа их защищённости: Автореф. дис. канд. техн. наук: 05.13.19. – Брянск, 2013. – 19 с.

7. Моляков, А. С. Модели и метод противодействия скрытым угрозам информационной безопасности в среде облачных вычислений: Автореф. дис. канд. техн. наук: 05.13.19. – Санкт-Петербург, 2014. – 19 с.

8. Асмолов, Т. А. Защита информационных систем музейных и библиотечных фондов на основе решений задач комбинаторной оптимизации: Автореф. дис. канд. техн. наук: 05.13.19. – Москва, 2012. – 24 с.

9. SAS 70 OVERVIEW [Электронный ресурс]. – Режим доступа: sas70.com/sas70_overview.html, свободный. – Загл. с экрана (дата обращения: 14.05.2021).

10. ISO/IEC 27001: 2005 Information technology – Security techniques – Information security management systems – Requirements (IDT) [Электронный ре-

сурс]. – Режим доступа: http://www.gociss.ru/doc/13.GOST R ISO MEK 27001-2006.pdf, свободный. – Загл. с экрана (дата обращения: 14.05.2021).

11. Закон «О персональных данных»: Федеральный Закон РФ от 08.07.2006.

12. Защита информации. Требования по защите информации, обрабатываемой с использованием технологии виртуализации. Общие положения. [Электронный ресурс]: ГОСТ Р 56938-2016. – Введ. 2016-06-01.

13. Требования по защите информации, обрабатываемой с использованием технологий «облачных вычислений». [Электронный ресурс]: Проект ГОСТ.

14. The Seven Standards of Cloud Computing Service Delivery [Электронный ресурс]. – Режим доступа: SalesForce.com

15. Симоненкова, А. Н. Безопасность информационных технологий / Д. С. Симоненкова, А. Н. Велигура. // Эталонные модели информационных систем, построенных с использованием технологий облачных вычислений. – 2013. – №3 – С.28-32

16. Marinescu, Dan C. Cloud Computing: Theory and Practice / Dan C. Marinescu – University of Central Florida, Orlando – Morgan Kaufmann, 2013. – 416 с.

17. Application Package Standard [Электронный ресурс]. – Режим доступа: http://apsstandard.org/, свободный. – Загл. с экрана (дата обращения: 25.05.2021).

18. Алеексеев, П.Антивирусы. Настраиваем защиту компьютера от вирусов / П. Алеексеев, Д. Козлов, Р. Прокди – СПб: Наука и Техника – 2014. – 419 с

19. Талалаев, А. А. Распределённая система защиты облачных вычислений от сетевых атак. / А. А. Талалаев // Вестник СибГУТИ. – 2013 – №3. – С. 46-62.

20. Ивонин, П. В. Безопасность информационных технологий/ П.В.Ивонин // Безопасность облака в деталях. – 2013. – №2. – С. 37-40

21. Bethencourt, J. Ciphertext-policy attribute – based encryption / J. Bethencourt, A. Sahai, B. Waters. // In SP ’07: Proceedings of the 2007 IEEE Symposium on Security and Privacy, 2007. – P. 321-334

22. Гатчин, Ю. А. Теория информационной безопасности и методология защиты информации / Ю. А. Гатчин, В. В. Сухостат – СПб.: СПбГУ ИТМО, 2010. – 98 с.

23. Кирсанов, С. В. Метод оценки угроз информационной безопасности АСУ ТП газовой отрасли / С. В. Кирсанов // Доклады ТУСУРа. – 2013. – № 2 (28). – С. 112-115.

24. Шабуров, А. С. Моделирование оценки угроз безопасности информационных систем персональных данных / А. С. Шабуров, С. А. Юшкова, А. В. Бодерко А.В. // Вестник ПНИПУ – 2013. – № 7.

25. Плетнев, П. В. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса/ П. В. Плетнев, В. М. Белов // Доклады ТУСУРа. – 2012. – Т. 1, № 2. – С. 83-86.

26. Зыков, В. Д. Модели и средства обеспечения управления информационной безопасностью медицинских информационных систем: Автореф. дис. канд. техн. наук: 05.13.19. – Томск, 2010. – 26 с.

27. Савельева, А. А. Модели и методы комплексной оценки аппаратно-программных средств обеспечения конфиденциальности и целостности информации: Автореф. дис. канд. техн. наук: 05.13.19. – Москва, 2011. – 18 с.

28. Ngenzi, A. Applying mathematical models in cloud computing: A survey / A. Ngenzi // Department of Computer Science Engineering–School of Engineering. Jain University. – 2014. – Vol. 16. – P 36-46.

29. Azab, M. Toward Smart Moving Target Defense for Linux Container Resiliency / M. Azab, M. Bassem, A. S. Abed, M. Eltoweissy // Proceedings of the 41st IEEE Conference on Local Computer Networks, 2016.

30. Maochao, X. Cyber Epidemic Models with Dependences / X. Maochao, D. Gaofeng, X. Shouhuai // Internet Mathematics. – 2015. – Vol. 11. – P. 62-92.

31. Shouhuai, X. A Stochastic Model of Active Cyber Defense Dynamics / X. Shouhuai, L. Wenlian, L. Hualun. // Internet Mathematics. – 2015. – Vol. 11. – P. 23-61.

32. Кацупеев, А. А. Модификация математической модели выбора опти-

мальной стратегии информационной защиты распределённых систем / А. А. Кацупеев, Е. А. Щербакова, С. П. Воробьёв, Р. К. Литвяк // Инженерный вестник Дона: электрон. журн. – 2017. – № 1.

33. Security Intelligence Report 2017 [Электронный ресурс]. – Режим доступа: https://www.microsoft.com/en-us/security/mtenigence-report, свободный. – Загл. с экрана (дата обращения: 28.12.2020).

34. Hi-Tech Crime Trends 2017 [Электронный ресурс]. – Режим доступа: https://www.group-ib.ru/resources/threat-research/2017-report.html, свободный. – Загл. с экрана (дата обращения: 28.04.2020).

35. AV-Test Security Report 2016/2017 [Электронный ресурс]. – Режим доступа: https://www.av-test.org/fileadmin/pdf/security_report/AVTEST_Security_Report_2016-2017.pdf, свободный. – Загл. с экрана (дата обращения: 28.04.2018).

36. The Reign of Ransomware 2016 [Электронный ресурс]. – Режим доступа: https://www.trendmicro.com/vinfo/us/security/research-andanalysis/threat-reports/roundup/the-reign-of-ransomware, свободный. – Загл. с экрана (дата обращения: 28.04.2018).

ПРИЛОЖЕНИЕ А

Листинг программы

(обязательное)

Программная реализация предложенных моделей и алгоритмов, реализующих задачу поиска оптимальной стратегии формирования информационной безопасности распределённых систем, выполнена на языке C++ в среде Microsoft Visual Studio 2015. Концепция программного обеспечения заключается в том, что на основе имеющихся архитектуры системы и совокупности классов и средств защиты информации производится выбор оптимального варианта размещения средств защиты информации. Программный продукт содержит в себе следующие модули: модуль ввода данных, с которыми программа будет осуществлять работу, модуль настроек параметров алгоритма и модуль расчета оптимальной архитектуры средств защиты.

В качестве начальных данных используются файлы с указанными в них характеристиками угроз, механизмов противодействия им и узлов облачной системы.

Так как программа довольно громоздка, то приводится только код основной части программы.

```
#include <iostream>
#include <fstream>
#include <iomanip>
#include <string>
#include <cmath>
#include "stdafix.h"
using namespace std;

struct Dangers
{
	string name;
	double ver_0;// изначальная вероятность реализации угрозы
	double ver_1;// переоцененная вероятность реализации угрозы
	double damage;
};

struct defenders_classes
```

```
{
	string name;
	double coust;// стоимость средства защиты
	double effectivity;// эфективность средства защиты
	double usel; // узел где оно будет установлено
};

struct points_classes
{
	string name;
	double count;// количество узлов
	double damage;
};

void init(double *m1, int n)
{
	m1 = new double[n];
}

void init(double **m1, int n)
{
	m1 = new double *[n];
	for (int i = 0; i < n; i++)
	{
		m1[i] = new double[n];
	}
}

void init(double ***m1, int n)
{
	m1 = new double **[n];
	for (int i = 0; i < n; i++)
	{
		m1[i] = new double *[n];
		for (int j = 0; j < n; j++)
		{
			m1[i][j] = new double[n];
		}
	}
}

void full(double *m, string s);
void full(double **m, string s);
void full(double ***m, string s);

void main()
{
	double ***E=0;
	double ***x=0;
	double ***DRDC=0;
	double ***PRDC=0;
	double ***IND=0;
```

```
double **KS=0;
double **DMG=0;
double **P=0;
double *CNT=0;
double *KPR=0;


int CCOUNT = 5;
int DCOUNT = 5;
int OCOUNT = 5;
int NCOUNT = 5;
int KCOUNT = 5;


init(KS, KCOUNT);
init(CNT, KCOUNT);
init(E, KCOUNT);
init(x, KCOUNT);
init(DRDC, KCOUNT);
init(PRDC, KCOUNT);
init(IND, KCOUNT);

init(DMG, KCOUNT);
init(P, KCOUNT);

init(KPR, KCOUNT);


full(KS, KCOUNT);
full(E, KCOUNT);
full(x, KCOUNT);
full(DRDC, KCOUNT);
full(PRDC, KCOUNT);
full(IND, KCOUNT);

full(DMG, KCOUNT);
full(P, KCOUNT);
full(CNT, KCOUNT);
full(KPR, KCOUNT);

double res = 0;
for (int i = 0; i <= KCOUNT; i++)
{
        double temp_2 = 0;

        for (int j = 0; j <= DCOUNT; j++)
        {
                double temp_1 = 0;

                for (int m = 0; m <= NCOUNT; m++)
                {
                        for (int z = 0; z <= OCOUNT; z++)
```

```
                                        {
                                                double temp_0 = 0;
                                                for (int l = 0; l <= CCOUNT; l++)
                                                {
                                                        temp_0 += E[m][l][z] * x[m][l][i] * (1 +
KS[m][l]);
                                                }

                                                temp_1 *= KPR[i] *
IND[m][z][j]*PRDC[m][z][j]*temp_0;
                                        }
                                }


                                double temp_4 = 0;
                                for (int m = 0; m <= NCOUNT; m++)
                                {
                                        for (int z = 0; z <= OCOUNT; z++)
                                        {
                                                double temp_3 = 0;
                                                for (int l = 0; l <= CCOUNT; l++)
                                                {
                                                        temp_3 += E[m][l][z] * x[m][l][i] * (1 +
KS[m][l]);
                                                }

                                                temp_4 *= KPR[i] * IND[m][z][j] * DRDC[m][z][j] *
temp_3;
                                        }
                                }

                                temp_2 += P[i][j] - P[i][j] * temp_1*(DMG[i][j]-temp_4);
                        }

                        res = res+CNT[i]*temp_2;
                }

                cout << "Ущерб системе:\t"<<res << endl;
                system("pause");
        }
```