1.2 Элементы методологии управления безопасностью распределенных ИТ-инфраструктур с минимизацией энергопотребления

1.2.1 Мотивация и актуальность исследований

В процессе проектирования и разработки современных распределенных ИТ-инфраструктур на основе Web-, Cloud-, IoT- (Internet of Things) технологий с использованием компонентно-ориентированной парадигмы возникает противоречие между нарастающим спектром и интенсивностью реализации угроз и уровнем развития существующих методов анализа узявимостей, оценивания влияния на готовность, системной защиты и управления рисками успешных вторжений.

Развитие и внедрение энергоэффективных технологий и Green-вычислений всячески стимулируют переход ИТ-инфраструктур на облачные платформы, позволяющие в полной мере реализовать заложенные в инфраструктуру Green-Cloud возможности. На данный момент для многих ИТ-инфраструктур переход на облачные технологии ограничен на законодательном уровне в силу вопросов защиты и безопасности информации.

На международном уровне вопросы стандартизации безопасности облачных технологий активно развивает подкомитет JTC 1 SC 27 ISO/IEC, который ответствен за вопросы информационной безопасности. Следует выделить следующие стандарты этого подкомитета:

- проект стандарта ISO/IEC 27017 «Информационные технологии – Руководство по мерам информационной безопасности для использования сервисами облачных вычислений, основанное на стандарте ISO/IEC 27002» [1];

- стандарт ISO/IEC 27040:2015 «Информационные технологии – Безопасность хранения данных» [2];

- стандарт ISO/IEC 27018:2014 «Свод практик по мерам защиты персональных данных при оказании публичных облачных услуг» [3].

Этот подкомитет также активно взаимодействует по общим вопросам с подкомитетом JTC 1 SC 38 ISO/IEC, среди стандартов которого стоит отметить:

- ISO/IEC 17788:2014 «Информационные технологии – Распределенные прикладные платформы и сервисы – Облачные вычисления – Общие положения и словарь» [4];

- ISO/IEC 17789:2014 «Информационные технологии – Облачные вычисления – Эталонная архитектура» [5].

Следует отметить, что другая стандартообразующая организация международного уровня – ITU – публикует рекомендации, практически идентичные стандартам ISO/IEC. Информационной безопасности посвящены рекомендации серии ITU.X [5,5], а облачным технологиям – рекомендации серии ITU.Y. Практика такого дублирования направлена на сокращение сроков утверждения стандартов на национальном уровне.

Ряд национальных стандартообразующих органов (например, Североамериканский институт стандартов NIST, Министерство обороны США DoD [5]), а также международных консорциумов и форумов (например, Cloud Security Alliance) внедряют руководящие документы, опережающие международные стандарты в соответствующих направлениях.

Несмотря на активное стремление международных и национальных органов стандартизации, сроки разработки, утверждения и внедрения соответствующих стандартов на законодательном уровне занимают несколько лет.

В такой ситуации можно, естественно, до принятия соответствующих нормативных документов, продолжать использовать сертифицированную по требованиям информационной безопасности старую энергонеэфетивную ИТ-инфраструктуру. Но такая позиция имеет следующие недостатки: неэффективное использование энергоресурсов, увеличение затрат на обслуживание локального парка серверов и неготовность к миграции в облачную среду на момент принятия согласующих нормативных документов.

Актуальность исследований обосновывается возможностью функциональной декомпозиции ИТ-инфраструктуры на отдельные компоненты и сервисы, часть из которых можно перенести в облачную структуру не нарушая требований к информационной безопасности и ее защите.

1.2.2 Задачи и цели исследований

Основной задачей является разработка методологии управления безопасностью распределённых ИТ-инфраструктур с минимизацией энергопотребления. Целью исследования является повышение точности и адекватности математических и имитационных моделей распределенных ИТ-инфраструктур для систем с повышенными требованиями к надежности и безопасности (security) при изменении их параметров на различных этапах жизненного цикла.

Для достижения поставленной цели были решены следующие задачи:

а) проведен анализ существующих концепций развертывания ИТ-инфраструктур с активным использованием арендуемых энергоэфективных ресурсов Web-, Cloud-, IoT-технологий;

б) проведен анализ существующих методов оценки и обеспечения безопасности распределенных ИТ-инфраструктур и их компонент;

в) проведен анализ нормативной базы в области регулирования информационной безопасности распределенных ИТ-инфраструктур;

г) проведен анализ возможных угроз и уязвимостей компонент распределенных ИТ-инфраструктур с определением степени их критичности;

д) разработана методология управления безопасностью и энергоэффективностью распределенных ИТ-инфраструктур.

1.2.3 Сущность методологии управления безопасностью распределенных ИТ-инфраструктур с минимизацией энергопотребления

Методология управления безопасностью распределенных ИТ-инфраструктур с минимизацией энергопотребления базируется на использовании системы принципов, объединенных общей концепцией (рис. 1.1).

Начало исследования посвящено дальнейшему развитию ранее применявшейся методологии обеспечения и сертификации безопасности информационных систем и технологий. В качестве дальнейшего развития данной методологии выделены новые принципы, модели, методы и информационные технологии. При разработке методологии использована нормативная база. Был выполнен анализ формальных и риск-ориентированных подходов к оценке функциональной и информационной безопасности, выявлены и сформулированы присущие им недостатки.

Также были определены основные направления развертывания и эксплуатации Green – центров обработки данных (ЦОД). С одной стороны, применение дорогостоящих передовых технологий позволяет сократить энергозатраты ЦОД, с другой стороны, их окупаемость зависит от эффективного привлечения клиентов к использованию ресурсов. Применение Green-Cloud позволяет строить ИТ-инфраструктуру на основе дорогостоящих энергоэффективных решений, но при этом оплачивать только фактически используемые услуги/виртуальные ресурсы (а не всю аппаратную инфраструктуру ЦОД).

Концепция управления безопасностью при минимизации энергопотребления развивается применительно к сложным системам, построенным на принципах распределенной и динамической архитектуры, и формулируется как концепция гарантирования и управления информационной безопасностью ИТ-инфраструктур по фактическому состоянию при минимизации их энергопотребления.



Рисунок 1.1 – Концепция управления безопасностью и энергоэффективностью распределенных ИТ-инфраструктур

Разработанные элементы методологии реализуется посредством формулирования (разработки) и использования следующих принципов:

а) принцип динамического компонентно-параметрического конфигурирования распределенных ИТ-инфраструктур и их информационных систем с минимизацией энергопотребления, который реализуется посредством формального теоретико-множественного представления динамики изменения входных и выходных параметров ИТ-инфраструктур, их функциональных характеристик и архитектурных решений, а также разработки и применения моделей и методов оценки рисков на этапах развертывания и сертификации; на рис. 1.2 в качестве примера представлены варианты обработки задач ИТ-инфраструктуры с различным уровнем критичности в приватной, публичной и гибридной облачной среде;



Рисунок 1.2 – Варианты обработки потока задач при переносе их в публичный Cloud, (ТА-подмножество задач с максимальным уровнем критичности, ТВ-подмножество задач с повышенным уровнем критичности, ТС-подмножество задач с обычным уровнем критичности, ТU-подмножество некритичных для ИБ задач)

б) принцип наследования характеристик, методов и моделей надежности, функциональной и информационной безопасности, суть которого заключается в применении оценочных подходов к свойствам информационной безопасности и категорирования ИТ-инфраструктур на основании значений оцененных показателей, имеющих переменный во времени вероятностный характер;

в) принцип динамического мониторинга и прогнозирования параметров уязвимостей компонент распределенных ИТ-инфраструктур для оценивания и минимизации рисков атак на них, для реализации которого требуется разработка подхода к исследованию влияния внешних факторов на вероятность проведения атаки и к объединению инструментариев аналитических аппаратов предсказания временных параметров проявления уязвимостей, проведения атак и изменения внешних факторов ИТ-проекта;

г) принцип управляемой деградации качества распределенных ИТ-инфраструктур в условиях агрессивной среды и потери компонент, для реализации которого требуется разработать:

– теоретико-множественное описание стратегии обновления и тестирования работающих компонент с возможным откатом к прежней версии;

– модель допустимых потерь качества обслуживания и их влияния на рейтинговые показатели ИТ-проекта в силу проведения обновлений ПО, тестирования нового функционала, проверок аудита ИБ.

1.2.4 Научная новизна полученных результатов

Научная новизна полученных результатов состоит в дальнейшем развитии методологии управления информационной безопасностью ИТ-инфраструктур по фактическому состоянию, которая, в отличие от известных, базируется на анализе, формализованном представлении и выделении методов, функциональных средств и компонент инфраструктуры с заданным уровнем критичности для информационной безопасности. В рамках методологии:

– предложен принцип динамического компонентно-параметрического конфигурирования распределенных ИТ-инфраструктур и информационных систем, который основан на формальном теоретико-множественном представлении динамики изменения входных и выходных параметров ИТ-инфраструктур, их функциональных характеристик и архитектурных решений; а также разработки и применения моделей и методов оценки рисков на этапах развертывания и сертификации;

– предложен принцип наследования характеристик, методов и моделей надежности, функциональной и информационной безопасности, который отличается унификацией процедур формализации и оценивания параметров отказов и уязвимостей компонент распределенных ИТ-инфраструктур;

– предложен принцип динамического мониторинга и прогнозирования параметров уязвимостей компонент ИТ-инфраструктуры, который учитывает влияние внешних факторов на вероятность проведения атаки и объединение инструментариев аналитических аппаратов предсказания временных параметров проявления уязвимостей, проведения атак и изменения внешних факторов ИТ-проекта;

– усовершенствован принцип управляемой деградации качества в условиях агрессивной среды и потери компонент активов на основе использования стратегии обновления и тестирования работающих компонент с возможным откатом к прежней версии.

Предложенная методология позволяет обеспечить снижение рисков угроз информационной безопасности активам доступности компонент ИТ-инфраструктуры на этапах их развертывания и миграции в облачной среде.

1.2.5 Практическое значение полученных результатов

Практическое значение полученных результатов определяется тем, что они:

– позволяют повысить полноту оценки и анализа информационной безопасности распределенных ИТ-инфраструктур;

– являются основой для создания информационной технологии поддержки процессов управления безопасностью при оценке и выборе вариантов Web-, Cloud – ИТ-инфраструктур, их аудита и сертификации.

1.2.6 Апробация полученных результатов

Результаты исследований апробированы:

– при выполнении международного проекта TEMPUS-GREENCO;

– в учебном процессе кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ» и кафедры компьютерной инженерии Полтавского Национального технического университета им. Юрия Кондратюка.

Результаты научных исследований докладывались и обсуждались на кафедре компьютерных систем и сетей Национального аэрокосмического университета «ХАИ», а также на международных научных конференциях: 11th International Conference, ICTERI 2015 (г. Львов, Украина, 2015), 10th International Conference on Dependability and Complex Systems DepCoS-RELCOMEX (Brunów, Poland, 2015), 5 международной научно-технической конференции «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління» (г. Полтава, Украина, 2015).