Содержание

ВВЕДЕНИЕ

Актуальность исследования. Развитие информационных технологий, их проникновение во все сферы человеческой деятельности приводит к тому, что проблемы информационной безопасности с каждым годом становятся всѐ более и более актуальными – и одновременно более сложными.

Результаты и перспективы информатизации общества свидетельствуют о наличии устойчивой тенденции интегрирования компьютерных средств и средств связи в рамках нового класса систем – компьютерных систем (КС) [43,64,88]. Системы данного класса с каждым днем находят все более широкое применение в [12,31,38,44,59], самых различных областях общественной жизни: начиная от деятельности телекоммуникационных компаний в рамках отдельных регионов и заканчивая деятельностью важнейших государственных институтов, таких как органы государственного управления, обороны, внутренних дел и т.д. При этом, [49] неконтролируемый рост числа абонентов КС, увеличение объемов хранимой и передаваемой ими информации, их территориальная распределенность приводит к возрастанию потенциально возможного количества преднамеренных и непреднамеренных нарушений безопасности, возможных каналов несанкционированного проникновения в сети с целью чтения, копирования, подделки программного обеспечения, текстовой и другой информации. При этом по сравнению с изолированными (автономными) автоматизированными системами в разветвленной КС появляются дополнительные возможности нарушения безопасности информации. [12,32]

Технологии непрерывно совершенствуются, а вместе с ними меняются и практические методы обеспечения информационной безопасности. Отсюда, все более актуальной становится проблема обеспечения безопасности КС, под которой понимается состояние информации, технических средств и технологии, характеризующееся свойствами конфиденциальности, целостности и доступности информации.

КС, в силу своего исторического развития, представляют собой распределенные, сложные структуры. КС представляет собой многоуровневую

иерархическую структуру, включающую в себя множество узлов, связанных между собою определенным образом [28] Свойство уязвимости присуще такой конструкции, в силу присутствия многочисленных узлов и связей между ними.

Универсальных методов защиты не существует, поэтому во многом успех при построении механизмов безопасности для реальной системы будет зависеть от еѐ индивидуальных особенностей, учѐт которых плохо поддаѐтся формализации. Поэтому часто информационную безопасность рассматривают как некую совокупность неформальных рекомендаций по построению систем защиты информации того или иного типа. [28] За практическими приѐмами построения систем защиты лежат общие закономерности, которые не зависят от технических особенностей их реализации. Очевидно, что решение проблемы обеспечения безопасности КС должно осуществляться системно на основе оценки технологии защиты информации, передачи ее по каналам связи, и не должно рассматриваться как чисто техническая задача, которая может быть решена попутно с разработкой элементов КС. [3,4]

Изучение свойств распределений экстремальных значений в течение долгого времени находилось несколько в стороне от основных направлений статистической теории распределений. В настоящее время теория распределения экстремальных значений является составной частью многих естественнонаучных дисциплин. Распределениями экстремальных значений первоначально интересовались абстрактные вероятностники, да специалисты в прикладных областях — инженеры и гидрологи. Только с недавних пор эти распределения вошли в сферу существенных интересов специалистов по статистике. [81]

Распределение экстремальных значений основывается на предельных распределениях для максимумов или минимумов (крайние значения) независимых, одинаково распределенных случайных величин, по мере увеличения размера выборки. Теория экстремальных значений моделирует события, которые происходят с очень малой вероятностью. Отсюда следует полезность в моделировании рисков для событий с малой вероятностью.

При построении риск-модели КС на основе переменных состояний защищенности (ПСЗ) статистическому временному ряду свойственен большой объем выборки и определенная периодичность колебания, вследствие работы персонала и пользователей КС. В свою очередь вероятность возникновения ущерба является относительно малой. Из этого следует, что для построения риск-модели КС целесообразно использовать экстремальные значения ПСЗ, что позволит сократить объем обрабатываемой информации и построить риск-модель на основе большего промежутка времени, а следовательно и большей точностью.

Степень научной разработанности. Существует достаточное большое количество работ, в которых осуществляется попытка построения риск-модели КС. При этом в них может рассматриваться определенный тип угроз и атак на данную КС, плотности вероятности распределения ущербов в этих системах распределены по определенному закону. Тем не менее, исследование возможности применения законов распределений экстремальных значений для построения риск-модели является актуальной задачей. Таким образом, исходя из актуальности и степени научной разработанности данной проблемы, можно сделать вывод о целесообразности проведения исследований в данном направлении.

Цели и задачи исследования. Целью дипломной работы является разработка и исследование риск-моделей компьютерных систем (КС) переменные состояния защищенности которых являются периодическими и имеют свойства цикличности, и распределены на основе законов, описывающих распределение экстремальных значений состояния информационной безопасности.

Для достижения этой цели необходимо решить следующие задачи:

1. Определить множество численных характеристик состояния информационной безопасности, характеризующих работу КС с периодическими переменными состояния защищенности (ПСЗ) с позиции обеспечения конфиденциальности, целостности и доступности информации и нарушение которых является признаком возникновения инцедентов информационной безопасности;

2. Построить аналитические выражения для оценки наносимого ущерба в зависимости от значения порога безопасности переменного состояния;

3. Разработать методику риск-анализа КС с периодическими ПСЗ на основе законов Гумбеля и Мизеса;

4. Разработать алгоритм минимизации риска КС с периодическими ПСЗ на основе законов Гумбеля и Мизеса.

Объектом исследования являются периодические переменные состояния защищенности компьютерных систем (КС) с заданными порогами допустимых значений экстремумов, которые не превышают заданного порогового уровня безопасности.

Предметом исследования является риск-анализ состояния защищенности компьютерных систем (КС) в условиях приближения экстремальных значений периодических переменных состояний к порогам безопасности.

Методы исследования. Для решения поставленных задач предполагается использовать методы системного анализа и математического моделирования, основанные на теории вероятностей и математической статистики, применительно к описанию распределений экстремальных значений переменных состояний защищенности.

Степень обоснованности научных положения, выводов и рекомендаций, сформулированных в дипломной работе предполагается обеспечить рациональным и обоснованным применением математических методов в приложении обозначенному предмету исследования.

Научная новизна исследования предположительно будет заключаться в:

1. Сформированном множестве числовых показателей ИБ КС с периодическими ПСЗ.

2. Разработанной риск-модели КС с периодическими переменными состоя, основанной на законах, описывающих распределение экстремальных значений переменных состояний защищенности КС с периодическими ПСЗ.

3. Методике прогнозирования возможных экстремальных значений числовых показателей ИБ КС с периодическими ПСЗ.

Практическая ценность работы заключается в том, что:

1. Рассмотренный подход, учитывающий построение риск-моделей КС с периодическими ПСЗ на основе экстремальных значений числовых показателей защищенности КС, позволяет повысить точность оценки и прогнозирования риска в КС по сравнению с методом экспертных оценок.

2. Полученные риск-модели КС с периодическими ПСЗ могут быть использованы для проектирования и построения компьютерных систем, устойчивых к инцидентам ИБ, влекущим за собой превышение допустимого порогового уровня ПСЗ.

3. Разработанная методология оценивания и созданный на ее основе алгоритм минимизации уровня риска позволяют измерить риски в режиме реального времени, снизить риски для уязвимых узлов системы, диапазон ущербов для системы в целом, а также осуществлять их краткосрочное прогнозирование, повышая точность и быстродействие системы управления в КС.

ЗАКЛЮЧЕНИЕ

Дипломная работа посвящена разработке и исследованию риск-моделей информационно-телекоммуникационных систем, а именно компьютерных систем с периодическими переменными состояний защищенности. В ходе ее выполнения были получены следующие основные результаты:

1. Рассмотрены и проанализированы законы распределения Гумбеля и Мизеса из семейства законов распределений экстремальных значений. Выявлены области применения этих распределений для задач информационной безопасности компьютерных систем с использование переменных состояний защищенности.

2. Сформировано множество числовых показателей ИБ компьютерных систем, для которых характерно свойство периодичности.

3. При решении задач, применительно к проблематике работы, результативно использовались методы численные методы расчета и анализа, методы теории рисков, теории вероятности и системного анализа.

4. Предложена оценка риска компьютерных систем с периодическими ПСЗ не превышающими заданных порогов безопасности, распределенными по законам Гумбеля и Мизеса является перспективным подходом для улучшения качества построения риск-моделей КС с периодическими ПСЗ, регулирования рисков и повышения защищенности компьютерных систем.

5. Получены аналитические выражения риск-моделей компонент компьютерных систем, плотность вероятности наступления ущербов в которых распределены по законам Гумбеля и Мизеса.

6. Исследованы аналитические риск-модели компьютерных систем, с периодическими ПСЗ, в которых ПСЗ не превышают заданный пороговый уровень. Получены аналитические выражения для расчета параметров риска для распределений Гумбеля и Мизеса, нахождения риска в диапазоне ущербов, оценка интегрального риска системы, проведена дискретизация риска. Проведена оценка и регулирование общего риска системы.

7. Получены риск-модели КС с периодическими ПСЗ, которые могут быть полезными для проектирования и построения компьютерных систем, устойчивых к

инцидентам ИБ, влекущих за собой превышение допустимого порогового уровня ПСЗ.

8. Найдены выражения для определения параметров чувствительности рисков КС с периодическими переменными состояний защищенности, а также построены уравнения движения риска КС с периодическими ПСЗ распределенными по законам Гумбеля и Мизеса.

9. На основе оценки риска компьютерных систем, состоящих из двух компонентов, была произведена оценка рисков для компьютерных систем, состоящих из n компонентов в общем виде, в компонентах которых плотность вероятности наступления ущебра имеют распределения Гумбеля и Мизеса.

10. Исследованы методики и алгоритмы управления информационными рисками системы, базирующиеся на основе стратегии оптимизационного снижения риска, и приведена адаптация алгоритма наискорейшего спуска для решения данной оптимизационной стратегии.

11. Разработана методология оценивания и созданный на ее основе алгоритм минимизации уровня риска позволяют измерить риски в режиме реального времени, снизить риски для уязвимых узлов системы, диапазон ущербов для системы в целом, а также осуществлять их краткосрочное прогнозирование, повышая точность и быстродействие системы управления в КС.

12. Проведена оценка экономических показателей эффективности разработанных риск-моделей компьютерных систем на основе периодических переменных состояний защищенности КС с заданными порогами допустимых значений экстремумов, не превышающих заданного порогового уровня безопасности.

Результаты исследований имеют солидную область применения.

Построенный математический аппарат, а также приведенные методики и алгоритмы управления риском позволят проектировать и строить компьютерные системы, устойчивые к инцидентам ИБ, и влекущим за собой превышения заданных допустимых порогов уровней ПСЗ, а также адекватные системы предупреждения и

защиты компьютерных систем в условия недетерминированных проявлений дестабилизирующих инцидентов ИБ.