Анализ возможных угроз и анализ рисков служит основой для обоснования выбора мер по обеспечению информационной безопасности ИТКС, которые должны быть осуществлены для снижения риска до приемлемого уровня. Риск-анализ позволяет всесторонне исследовать атакуемые ИТКС, оценить текущий уровень состояния ИБ, выявить уязвимые места в системе защиты, создать модели возможных угроз ИТКС, проверить правильность подбора и настройки средств защиты от реализации атак.

Вопрос выживаемости ИТКС является не менее актуальным и имеет не только теоретический, но и практический интерес. Так, например, ИТКС подвергаются массированным атакам со стороны недобросовестных конкурентов, их деятельность подвергается компрометации со стороны действующих аналогов. Поэтому при проведении риск-анализа, так же осуществляется оценка жизнестойкости подобных проектов ,ибо только при оценке вероятного ущерба возможно найти истинный риск «смертности» систем[11].

Таким образом, целью проведения такого анализа является разработка ряда методик, моделей и организационных документов, которые в дальнейшем могут явиться основой для построения защищенной ИТКС.

Из изложенного следует, что системное рассмотрение структуры ИТКС, механизмов реализации атак на компоненты ИТКС, которые обмениваются информацией посредством технологии Ethernet, позволит выявить основные временные и вероятные характеристики реализации угроз удаленного доступа, что, в свою очередь, позволит исследовать и разработать методику анализа информационных рисков и управления защищенностью ИТКС от воздействий угроз удаленного доступа к ееэлементам, при плотности вероятности отказов элементов ИТКС, распределенной по закону Гомпертца.

Цель и задачи исследования.

Целью данного исследования является оценка рисков и выживаемости, атакуемых ИТКС при плотности вероятности отказов их компонентов, распределенной по закону Гомперца.

Для достижения указанной цели предполагается решить следующие задачи:

1. Проанализировать состояние вопроса и уточнить предмет, объект, и методы исследования.

2. Построить аналитическую модель распределения ущерба в зависимости от времени.

3. Разработать аналитическую риск-модель для компонентов ИТКС, рассчитать основные параметры распределения риска.

4. Построить динамическую модель риска на основе функции чувствительности.

5. Провести анализ модели риска, включая случай многокомпонентного отказа.

Объектом исследования являются компоненты информационно-телекоммуникационные системы, в отношении которых реализуются атаки, оказывающие деструктивное воздействие на их компоненты.

Предметом исследования являются риски реализации деструктивных информационных воздействий на информационно-телекоммуникационные системы.

Методы исследования. В исследовательской работе применялись: методы из аппарата теории вероятности и математической статистики, теория графов, методы системного анализа, теории рисков, а так же теории надѐжности.

На защиту выносятся следующие основные положения работы:

1. Аналитическая риск-модель «смерти» компонент ИТКС, ущербы в которых, в результате дестабилизирующих факторов распределенных по закону Гомперца.

2. Динамическая риск-модель «смерти» компонент ИТКС.

Научная новизна результатов исследования. В настоящей работе получены следующие основные результаты, характеризующиеся научной новизной:

- разработана статистическая риск-модель атакуемой ИТКС, при плотности вероятности отказов ее компонентов, распределенной по закону Гомперца;

- разработана динамическая риск-модель атакуемой ИТКС, при плотности вероятности отказов ее компонентов, распределенной по закону Гомперца. Получена функция чувствительности;

- разработана модель распределения ущерба в зависимости от времени.

На защиту выносятся следующие основные положения работы:

1. Аналитические риск-модели для компонент ИТКС, ущербы в которых, в результате дестабилизирующих факторов распределенных по закону Гомперца.

2. Функция чувствительности и жизненный цикл ИТКС.

3.Рекомендации по повышению защищенности ИТКС, на которую производятся информационные атаки.

Практическая ценность работы заключается в том, что:

1. Полученные статическая и динамическая риск-модели могут быть использованы для построения в государственных и коммерческих организациях систем, устойчивых к сетевым атакам приводящих к полной утрате работоспособности, оценки эффективности обеспечения защиты от сетевых атак в данных организациях, выявления наиболее уязвимых к сетевым атакам ресурсам организаций.

2. Предложенные рекомендации по регулированию рисков позволяют снизить риски для наиболее уязвимых компонент систем, а также диапазон ущербов для системы в целом, что открывает возможности по повышению защищенности организаций от сетевых атак, использующих в своей работе сетевые технологии.