ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Количество реализуемых угроз постоянно возрастает, что говорит оширокихвозможностях для злоумышленников по осуществлению различныхдеструктивных воздействий [1,2].Увеличению количества атак способствуетразвитие сетевых структур[3].

Сетевая структура представляет собой иерархически выстроенную структуру, включающую в себя большое количество узлов, связанных между собою конкретным образом, состоящая из структурно-функциональных элементов рабочих (станций, серверов, сетевых устройств и каналов связи).

По мере эволюции подобных систем увеличивается их чувствительность к деструктивным воздействиям.Проявившееся противоречие достигнутого уровня развития указанных систем и уровня развития средств и мер обеспечения безопасности и устойчивости требует своего разрешения наиболее рациональным образом. В этом состоит философский аспект актуальности усилий, направленных на разработку теоретических основ живучести сетевых структур различного уровня и масштаба, а также способов реализации на практике знаний, добытых в ходе научного поиска [6].

Впервые в обиход понятие "живучесть" введено адмиралом С.О. Макаровым: "Живучесть – это способность корабля вести бой, имея повреждения в различных боевых частях" (1894 г.) [7], причем термины "живучесть" и "непотопляемость" были синонимами. Применительно к сетевым структурам живучесть можно трактовать, как способность системы выполнять основные свои функции, несмотря на полученные повреждения, либо адаптируясь к новым условиям[8].

Хорошо известен тот факт, что возрастание числа элементов сетевых структур приводит к увеличению вероятности нанесения ущерба со стороны злоумышленника при реализации атак, например таких, как DDoS-атака. Взять хотя бы для примера тот факт, что с увеличением клиентской базы на 10% QratorLabsв первой половине 2015 года с помощью собственного одноименного сервиса нейтрализовала 9457 DDoS-атак. В аналогичном периоде 2014 года эта цифра

составила 2896. Максимальное число атак в день, нейтрализованных сетью фильтрации трафика Qrator, увеличилось с 45 в первом полугодии 2014 до 127 в 2015 году. Также выросло и среднее количество DDoS в день — от 17 до 63, соответственно [9,10].На данный момент одним из перспективных подходов является метод анализа выживаемости[11,12].

В настоящее время задача анализа и синтеза сетевых структур является достаточно сложной ,поэтому часто для решения нужно проектировать отдельную модель. Исследования в этом направлении ведутся с середины 20 века, было предложено огромное количество подходов для решения указанных задач.

Основные подходы для оценки живучести применительно к сетевым структурам[15–20]:

1)вероятностные полиномиальные процедурные модели расчета;

2)процедурные модели, построенные с использованием искусственного интеллекта;

3)поточные модели.

Отыскание путей обеспечения живучести элементов сетевых структуртребует постановки и решения большого количества научно-технических задач синтеза живучести систем на этапе их создания, модернизации или усовершенствования. Особенно это актуально для 21 века – века высоких технологий, времени информационных войн и компьютерной зависимости ,когда информационные ресурсы нередко представляют собой большую ценность, чем ресурсы материальные,что очевидно, привело к увеличению числа атак на элементы сетевых структур. Таким образом, необходимо найти наиболее эффективные подходы к оценке работоспособности системы подобного рода. Одним из перспективных подходов является регулирование эффективностью защиты элементов сети и управление еѐ живучестью.

Отмеченное доказывает актуальность освоения и внедрения в практику основ живучести систем.

Степень научной разработанности

Касательно вопросов управления информационными рисками [1,3,22,23], в частностианализаживучести систем[22 – 29],методоврасчета[34– 38], а также особенностей применения моделей анализа[39–50], опубликовано огромное количество научных работ, которые дали толчок в развитии математических основ анализа и синтеза качественных характеристик сетевых структур [51–53]. Анализ этих и других работ позволяет выявить тенденцию постепенного перехода в оценке показателей живучести к более оптимальным, которыебазируются на моделях с учетом структурных и функциональных факторов [54–56].

Следует отметить, что практическое использование отмеченных выше работ нуждается в значительном исходном материале по стойкости элементов сетевых структур к вредоносным воздействиям и корректировки риск–анализа. Так, например, из риск–оценкивыживаемости исключен анализ величины ущерба и функции полезности, что недопустимо для корректного риск–анализа [57–61].

В данной работе делается попытка развития комплекса аналитических выражений: оценки смертности атакуемых объектов для всевозможных законов распределения плотности вероятности их гибели ;ущербов и пользы для различных функции полезности и разнообразных атакуемых объектов, что поможет оптимизировать ожидаемую эффективность защиты и живучесть атакуемых объектов.

Таким образом, произведенная оценка полезности системы, полученная в ходе анализа выживаемости, позволит найти истинный ущерб сетевых структур в условиях отказов компонентов и разработать эффективные методы по предотвращению деструктивных действий в результате вредоносных атак.

Объектом исследования является сетевая структура, как цель атак, направленных на элемент сети.

Предметом исследования является риска-анализ выживаемости элемента сетевой структуры для различных законов распределения его отказов.

Цель работы состоит в повышение живучести за счѐт создании аналитического и программного инструментария оценки жизнестойкости атакуемых элементов сетевых структур.

Методологическая, теоретическая и эмпирическая база исследования.

В работе используются методы системного анализа, теории вероятностей и математической статистики, математического анализа, методы теории рисков и экспертных оценок.

Для достижения поставленной цели необходимо решить следующие задачи:

1) Построение аналитических моделей оценки ущерба и пользы при отказах атакуемых элементов сетевых структур для различных аппроксимаций функции полезности.

2) Построение аналитических моделей оценки жизнестойкости атакуемых элементов сетевых структур для различных видов распределения вероятности (плотности вероятности) их отказа, включая дискретизацию по времени.

3) Алгоритмизация и программная реализация предложенных моделей, включая многовариантный расчет для всевозможных функций эффективности (полезности) и вероятности (плотности вероятности) отказа атакуемых элементов сетевых структур.

4) Регулирование эффективностью защиты элементов сети и управление еѐ живучестью.

Результаты, выносимые на защиту:

1) Аналитические модели оценки ущерба и пользы при отказах атакуемых элементов сетевых структур для различных функции полезности.

2) Аналитические модели оценки жизнестойкости атакуемых элементов сетевых структур для различных видов распределения вероятности (плотности вероятности) их отказа, включая дискретизацию по времени.

3) Алгоритмизация и программная реализация предложенных моделей, включая многовариантный расчет для всевозможных функций эффективности (полезности) и вероятности (плотности вероятности) отказа атакуемых элементов сетевых структур.

Новизна результатов:

1) В отличие от аналогов, учтено более полное множество функций полезности атакуемых элементов сетевых структур.

2)Получены оригинальные аналитические модели, охватывающие практически все известные виды распределений вероятности (плотности вероятности) их отказа ,включая дискретизацию по времени.

3) Получен и апробирован программный продукт, в отличие от аналогов ориентированный на многовариантные расчеты и оптимизацию для широкого многообразия функции полезности и вероятности (плотности вероятности) отказа атакуемых элементов сетевых структур.

Практическая ценность результатов:

1) Аналитические модели оценки ущерба и пользы при отказах атакуемых элементов сетевых структур для различных функции полезности открывают принципиально важные перспективы с точки зрения регулирования риска сетевых структур.

2) Из полученных аналитических моделей следует возможность многовариантного расчета и оптимизации риска выживаемости атакуемых сетей вплоть до синтеза с заданной живучестью.

3) Программный продукт может быть использован для риск–анализа элементов сетевых структур (серверы и т.д.), подвергающихся атакам в условиях информационного конфликта.

ЗАКЛЮЧЕНИЕ

В рамках данной работы были рассмотрены основные функции полезности, которые наиболее точно описывают период функционирования элемента сети или сетевой структуры в целом. Рассмотренные аппроксимации данных функций полезности позволяют проводить экспресс-анализ, когда время или ресурсы оператора ограничены.

Построенные аналитические модели оценки ущерба и пользы при отказах атакуемых элементов сетевых структур для различных функции полезности,помогут наиболее полно проводить анализ шансо–рисковой оценки.

В работе предлагаются аналитические оценки живучести для различных видов распределения отказов сетевых структур,где риск-анализ осуществлен в направлении: аналитической оценки ущерба через дискретизациюфункции полезности; отношение шанс-риск, показывающее ожидаемую эффективность защиты. Соответствующие аналитические выражения, полученные в работе, служат методической основой для риск–анализа систем различного профиля с точки зрения их возможного отказа.

Предложенная методика оценки жизнестойкости и эффективности отвечает данным требованиям и,безусловно, может быть эффективно применена на практике. В работе представлена алгоритмизация и программная реализация предложенных моделей, включая многовариантный расчет для всевозможных функций эффективности (полезности) и вероятности (плотности вероятности) отказа атакуемых элементов сетевых структур.Программа также содержит необходимый иллюстративный материал в виде графиков, качественно отражающих функции полезности, шанса и риска, живучести и эффективности.