Введение

Актуальность исследования.Обеспечение информационной безопасности – одна из главных задач любой современной организации. Фундаментом для построения системы управления информационной безопасностью являются процессы оценки и управления информационными рисками [1]. Значимость управления информационными рисками заключается в возможности, во-первых, прогнозировать в определенной степени наступление рискового события, во-вторых, заблаговременно принимать необходимые меры к снижению размера возможных неблагоприятных последствий[2].

Из-за неадекватной оценки рисков, связанных с осуществлением угроз информационной безопасности в современном высокотехнологичном обществе, государство, организации и отдельные личности несут весьма ощутимый ущерб [3]. Точность оценки рисков, связанных с осуществлением деятельности по информационной безопасности, является основной характеристикой профессиональной зрелости специалиста в предметной области. При отсутствии адекватной оценки рисков сложно решать вопрос о необходимости и достаточности того или иного набора мер по защите информации и их адекватности существующим рискам [4].

В данной дипломной работе предлагается проведение риск-оценки информационной устойчивости программных продуктов при воздействиях типа «троян».

«Троян» - программа (программный модуль), осуществляющая различные несанкционированные действия: сбор информации иее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях[5].

Программные продукты занимают промежуточное положение между вычислительными процессами низкого уровня (функционирование процессоров) и процессами высокого уровня – взаимодействие с оконечным оборудованием или пользователем. Поэтому программные продукты являются

определяющими элементами как для индикации нарушений нормальной работы процессора, так и для контроля в отношении оконечного оборудования или пользователя. Но программные продукты могут существовать только в контексте некоторой компьютерной системы, следовательно, риск-оценку информационной устойчивости программных продуктов необходимо рассматривать как риск-оценку (риск-анализ) информационной устойчивости компьютерной системы, в состав которой они входят.

Под информационной устойчивостью компьютерной системы будем понимать способность компьютерной системы эффективно реализовывать свои целевые функции, т.е. эффективно функционировать. При этом показателем устойчивости может выступать амплитуда отклонения риска компьютерной системы от некоторого заданного значения.

В настоящее время за счет существенного расширения номенклатуры и возможностей троянских программ эффективность средств защиты информации заметно снизилась. Поэтому вопрос оценки рисков, связанных с осуществлением троянских атак на компьютерную систему, является первоочередным и заслуживающим достаточного внимания.

Степень научной разработанности. Исследование вопросов взаимодействия троянских программ с компьютерными системами было начато с задержкой примерно в один год после появления данного класса информационных воздействий. При этом необходимо отметить, что вопросы принципиального построения и алгоритмов функционирования этих программных продуктов обсуждалось задолго до их появления на международной конференции в Киеве[6], в приватных конференциях сетей Fido, рассматривались в [7, 8]. В этих работах в той или иной степени анализировались вопросы взаимодействия средств информационных воздействий с элементами операционных платформ, однако, как таковых вопросов защиты не ставилось, что было обусловлено:

- замкнутостью концепций защиты на гармонизированные критерии «Оранжевой книги» и отсутствием формализованных моделей взаимодействия

хотяпроцесс реализации своих целевых функций этими воздействиями в операционной среде имеет достаточно много особенностей, которые, в ряде случаев, выходят за рамки основных положений и концепций, рассматриваемых в вышеперечисленных работах.

Поэтому проведение риск-оценки информационной устойчивости программных продуктов при воздействиях типа «троян» является актуальной и практически важной задачей.

Цель и задачи исследования. Цель настоящей работызаключается в построении адекватной вероятностной модели троянских атак на компьютерную систему, а также в разработкеметодики оценки и управления возникающими в данном случае информационными рисками компьютерной системы.

Для достижения поставленной цели необходимо решить следующие задачи:

- рассмотреть подходы к определению и классификацию троянских программ, способы их проникновения на компьютеры пользователей, а также их структуру;

- разработать и исследовать вероятностные модели троянских атак на компьютерную систему, из одного и нескольких источников;

- разработатьриск-модели компьютерной системы, подвергающейся троянским атакам из одного и нескольких источников и исследовать их с позиций теории чувствительности;

- разработать алгоритм управления рисками компьютерной системы, подвергающейся троянским атакам из одного и нескольких источников;

- произвести оценку экономической эффективности, а также расчет сметной стоимости и договорной цены проведенного исследования;

- рассмотреть исследуемую проблематику с точки зрения обеспечения безопасности жизнедеятельности.

Объект исследования. Объектом исследования в данной работе является компьютерная система, подвергающаяся троянским атакам, причем каждая такая атака может быть либо успешной, либо неуспешной.

Предмет исследования. Предметом исследования является риск-оценка (риск-анализ) информационной устойчивости атакуемой компьютерной системы.

Заключение

В дипломной работе получены следующие основные результаты:

1. Рассмотрены подходы к определению и классификация троянских программ, способы их проникновения на компьютеры пользователей, а также их структура. Для дальнейшего исследования среди троянских программ был выделен подкласс Backdoor, составляющий немногим менее трети всего класса (29,63%), так как представители данного подкласса обладают наибольшей функциональностью и являются наиболее изощренными и развитыми средствами информационного воздействия внутри рассматриваемого класса.

2. На основе показательного распределения разработаны и исследованы вероятностные модели троянских атак на компьютерную систему, из одного и нескольких источников.

3. Разработаны и исследованы с позиций теории чувствительности риск-модели компьютерной системы, подвергающейся троянским атакам из одного и нескольких источников. Процесс распределенной троянской атаки на компьютерную систему рассматривался в контексте рассылки с помощью ботнетовспам-писемс вложенными троянскими программами подкласса Backdoor на внутренний почтовый сервер системы. Были получены аналитические выражения функций чувствительности рисков компьютерной системы к изменению параметров троянских атак. В результате расчетов был сделан вывод, что нахождение аналитических выражений функций чувствительности рисков к изменению параметров троянских атак является ключевым моментом в процессе риск-анализа, и последующего нахожденияуравнений движения рисков. С помощью уравнений движения рисковбыло проанализировано влияние параметров вероятностных моделей распределенной и нераспределенной троянских атак на функции рисков компьютерной системы.

4.Разработан алгоритм управления рисками компьютерной системы, подвергающейся троянским атакам из одного и нескольких источников, основанный