Троянские программы распространяются людьми – как непосредственно загружаются в компьютерные системы злоумышленниками-инсайдерами, так и побуждают пользователей загружать и/или запускать их на своих системах.

Для достижения последнего, троянские программы помещаются злоумышленниками на открытые или индексируемые ресурсы (файл-серверы и системы файлообмена), носители информации, присылаются с помощью служб обмена сообщениями (например, электронной почтой), попадают на компьютер через бреши безопасности или загружаются самим пользователем с адресов полученных одним из перечисленных способов.

Иногда использование троянов является лишь частью спланированной многоступенчатой атаки на определенные компьютеры, сети или ресурсы [3, 12, 13].

Для маскировки троянская программа может имитировать имя и иконку существующей, несуществующей, или просто привлекательной программы, компонента, или файла данных (например картинки), как для запуска пользователем, так и для маскировки в системе своего присутствия.

Троянская программа может в той или иной мере имитировать или даже полноценно выполнять задачу, под которую она маскируется (в последнем случае вредоносный код встраивается злоумышленником в существующую программу).

Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера (например, троянские программы, разработанные для распределенных DoS-атак на удаленные ресурсы сети) [5].

Хакеры постоянно работают над повышением эффективности работы различных вредоносных программ, в том числе и троянов [5, 7, 8, 9, 12, 13, 35]. Следовательно, обеспечение информационной безопасности – одна из главных задач любой современной организации. Фундаментом для

построения системы управления информационной безопасностью являются процессы оценки и управления информационными рисками, значимость которых заключается в возможности, во-первых, прогнозировать в определенной степени наступление рискового события, во-вторых, заблаговременно принимать необходимые меры к снижению размера возможных неблагоприятных последствий [1, 2, 9,14, 15]. Поэтому тема диплома, посвящѐнная изучению тенденций развития троянов, и предотвращение ситуаций нанесения ими ущерба информационно-телекоммуникационной системе является актуальной.

Соответствие темы диплома специальности.

Данная работа посвящена изучению воздействий троянов на информационно-телекоммуникационные системы, предотвращению ситуаций нанесения ими ущерба ИТКС, т.е. обеспечению безопасности ИТКС. Поэтому можно сделать вывод о соответствии темы данной работы специальности Безопасность телекоммуникаций.

Объектом исследования являются информационно-телекоммуникационные системы подвергающиеся воздействиям типа «троян».

Предметом исследования является риск-оценка информационной устойчивости информационно-телекоммуникационных систем в условиях реализации воздействия типа «троян».

Цель и задачи исследования.

Целью настоящей работы является построение вероятностной модели троянских атак на информационно-телекоммуникационную систему и разработка методики оценки и управления возникающими в данном случае информационными рисками ИТКС.

Для реализации данной цели необходимо решить приведенные ниже задачи:

Заключение

Дипломный проект посвящен вопросам проведения исследований рисков информационной устойчивости информационно-телекоммуникационных систем в условиях реализации воздействия типа «троян».

В ходе выполнения работы были получены следующие основные результаты:

- проведена классификация троянских программ на основе обобщенных вариантов их структуры. На основе полученного результата выбрана вероятностная модель троянских программ;
- предложена вероятностная модель троянских атак на ИТКС. Эта модель была принята за математическую базу при проведении риск-анализа защищенности компьютерных систем, подвергающихся троянским атакам;
- предложена риск-модель компьютерной системы, подвергающейся троянским атакам. На основе риск-модели выбраны области эффективного управления рисками;
- предложен алгоритм управления рисками ИТКС, подвергающейся троянским атакам. При помощи предложенного алгоритма можно оптимизировать параметры ИТКС с целью минимизации рисков;
- оценена экономическая эффективность предложенного алгоритма управления рисками ИТКС, подвергающейся троянским атакам. Проведенная оценка показала экономическую целесообразность применения предложенных моделей и алгоритмов при исследовании риска ущерба ИТКС за счет троянских атак.