Содержание

8 (952) 106-88-60 vk.com/a.projectit a.projectit

projectIT

8 (952) 106-88-60 vk.com/a.projectit a.projectit

projectIT

Введение

Одним из главных направлений развития науки является внедрение информационных технологий во все сферы жизнедеятельности человека. На современном этапе развития обществаприоритетным является непрерывный процесс информатизации и совершенствования информационных технологий, что способствует постоянному расширению сферы внедрения коммуникационных и вычислительных систем, которые затрагивают все новые стороны жизни общества [2,8,24].

Открывая новые возможности перед человеком в модернизации различных технологических и управленческих процессов, повышении качества и эффективности работы, на АИС возлагается существенная ответственность за безопасность информации. Для правильной работы АИС осуществляется телекоммуникационное и информационное взаимодействие подсистем различного назначения (общего пользования, частных, производственных, ведомственных). Поддержание взаимосвязи отдельных территориально-распределенных подсистем внутри каждой из систем, а также между отдельными системами АИС происходит посредством постоянного предоставления услуг информационно-коммуникационного, аналитического характера, обеспечения информационной безопасности, администрирования единого информационно-телекоммуникационного пространства и средств безопасности. Данные, циркулирующие в АИС, должны быть не только актуальны и доступны, но и защищены от воздействия злоумышленников как изнутри, так и из вне[59,62,81].

В связи с этим важной задачей является обеспечение достаточной степени защищенности таких систем для их эффективного функционирования в условиях проявления внутренних и внешних информационных угроз и, в конечном счете, минимизации ущерба от деструктивных деяний[8,48].

Так как большинство АИС функционируют и проектируются с учетом использования в них технологии межсетевого взаимодействия, большое распространение получили удаленные атаки, направленные на реализацию угрозы

удаленного (с использованием протоколов сетевого взаимодействия) доступа, причины успеха которых кроются в самой инфраструктуре АИС.

Таким образом, становится актуальным использование «стратегии обмана» или отвлечения нарушителя на ложный информационный ресурс. Средства, которые реализуют такую стратегию, называются ложными информационными системами (ЛИС). Применяя с помощью ЛИС «стратегию обмана» нарушителя и отвлекая его на ложный информационный ресурс, можно не только не позволить злоумышленнику получить несанкционированный доступ к защищаемой информации, но и найти неизвестные ранее уязвимости[32,86].

Основными функциями таких систем являются привлечение и удержание внимания злоумышленников на ложных информационных целях, введение злоумышленников в заблуждение, обнаружение и фиксация действий нарушителей, их контроль, а также сбор и агрегация данных о действиях нарушителей из различных источников. ЛИС представляют собой программно-аппаратные средства обеспечения информационной безопасности, реализующие функции сокрытия и камуфляжа защищаемых информационных ресурсов, а также дезинформации нарушителей[24,87].

При использовании ЛИС важно знать, насколько эффективно можно обмануть с ее помощью нарушителя и при этом не создать сложностей для функционирования защищаемой АИС, так как значительный вычислительный ресурс может оказаться задействованным на обеспечение функционирования ЛИС[87].

Таким образом, необходимо разработать и провести риск-анализ актуальной и эффективной ЛИС, которая должна не только привести к срыву удаленных атак, но и не превышать вычислительных ресурсов информационной системы установленного уровня [8,48,63,95].

Степень проработанности темы

Необходимость обеспечения информационной безопасности требует поиска качественно новых подходов к решению многих технических и управленческих задач. Непредсказуемость атак не позволяет создать детерминированное описание процессов и возникающих от их реализации ущербов. Поэтому, при создании

защищенных АИС, вполне обоснованно применение ЛИС. [16, 46, 91, 96].

Таким образом, исходя из актуальности и степени научной разработанности проблемы нарастания ущерба реализации удаленных атак, можно сделать вывод о целесообразности проведения комплексных исследований в направлении анализа рисков реализации атак на АИС, защищенные посредством ЛИС, и в конечном итоге построения эффективных ЛИС.

Объектом исследования является автоматизированная информационная система, защищенная посредством ложной информационной системы.

Предметом исследования является риск-анализ и эффективность ложной информационной системы в условиях реализации удаленных атак.

Цели и задачи исследования.

Цель настоящей работы заключается в анализе эффективности и рисков, связанных с проведением удаленных атак на АИС, защищѐнных посредством ЛИС. Для реализации данной цели необходимо решить приведенные ниже задачи:

1. Провести анализ основных видов удаленных атак, воздействующих на АИС.
2. Разработать риск-модель АИС, компоненты которой подвергаются воздействию реализации удаленных атак, учитывающую наличие ЛИС;
3. Разработать итерационную модель работы ЛИС, отражающую этапы реализации удаленных атак на АИС;
4. Провести анализ живучести АИС и эффективности работы ЛИС при реализации атак удаленного доступа;
5. Осуществить соответствующее имитационное моделирование, выработать практические рекомендации по снижению информационных рисков в АИС и увеличению эффективности работы ЛИС;
5. Провести оценку экономической эффективности проведенного исследования;
6. Проанализировать возможные проблемы с учетом обеспечения безопасности жизнедеятельности.

Степень обоснованности научных положений, выводов и рекомендаций, сформулированных в дипломной работе, обеспечивается корректным

использованием математических методов в приложении обозначенному предмету исследования.

В исследовании предполагается использовать методы теории вероятности, методы математической статистики и статистического анализа, методы теории графов, методы теории Петри – Маркова, методы аналитического моделирования, методы теории рисков [12, 13, 26, 32].

Научная новизна исследования.

В настоящей работе получены следующие основные результаты, характеризующиеся научной новизной:

1. В исследовании процесса реализации удаленных атак на АИС, защищаемые посредством ЛИС, были учтены результаты их количественного и качественного развития.

2. В отличие от аналогичных работ, полученная риск-модель АИС, в отношении которой реализуются атаки удаленного доступа, учитывает особенности применения в системе защиты ЛИС.

3. Отличительной особенностью подхода к изучению безопасности автоматизированных информационных систем, в отношении которых реализуются атаки удаленного доступа является изучение живучести системы с разработкой методических рекомендаций по увеличению эффективности работы ЛИС.

Практическая ценность работы заключается в том, что:

1. Анализ основных видов удаленных атак, воздействующих на компоненты автоматизированных информационных систем, позволяет выявить наиболее опасные их виды и дает возможность уделить особое внимание разработке эффективной ЛИС.

2. Построенная риск-модель АИС отражает этапы реализации атак удаленного доступа и позволяет всесторонне оценивать процесс развития атаки.

3. Полученные выражения для живучести автоматизированных информационных систем на базе разработанной модели ущерба позволяют оценить эффективность защиты ЛИС от реализации атак удаленного доступа.