Содержание

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

Введение

Основной тенденцией в современном мире сегодня является переключение государств на инновационный путь развития. Этот путь подразумевает активное внедрение и широкое применение новейших и прогрессивных информационных технологий в следующих областях деятельности государств: экономике, финансах, промышленности, энергетики, национальной безопасности, транспорта, науки, здравоохранения, образования и многих других[35-37].

Однако повсеместное и свободное использование информационных технологий не представляется возможным без решения проблем собственной безопасности самих технологий. Это решение выражается не только в использовании и развитии традиционных методов и средств защиты информации, но и в образовании новых нестандартных подходов к обеспечению безопасности информационных ресурсов и систем. Примером такого подхода может служить систематическое поэтапное внедрение методов активной защиты, которые включают в себя методы дезинформации потенциального нарушителя, введения его в заблуждение. Частым случаем такого подхода является метод, при котором истинные информационные объекты, находящиеся в системе, защищают путем создания ложных информационных объектов, которые отвлекают на себя нарушителя. Метод дезинформирования потенциального нарушителя не является чем-то новым – он широко применяется военными при проведении специальных мероприятий. Смысл такого подхода достаточно прост: чем лучше реальные объекты замаскированы, тем меньше вероятность нанесения им ущерба. На данный момент данная тема широко изучается в зарубежных странах. В свете последних событий, происходящих в мире, метод введения в заблуждение потенциального противника приобретает всѐ большую актуальность и в Российской Федерации: Указ Президента №31с от 15 января 2013 года обязывает создать государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации[3].

В ИС всегда присутствует вероятность наличия неизвестных уязвимостей, а также уязвимостей в программном обеспечении самих средств защиты. В такой ситуации традиционные подходы к защите информации не могут обеспечить нужный уровень защиты информации при приемлемых финансовых затратах. Поэтому сегодня всѐ более актуальным становится применение ложных информационных систем (ЛИС), реализующих стратегию обмана. Целесообразность использования ЛИС в целях защиты информации отмечается в нормативном правовом акте ФСТЭК России приказе №17 от 11 февраля 2013 года «Требования по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». Реализуя защиту информационной системы с помощью ЛИС, тем самым отвлекая нарушителя на ложный информационный ресурс, можно не только защитить информационную систему, но и найти уязвимости этой системы, которые ранее были неизвестны[101].

ЛИС – это программно-аппаратные средства защиты информации, которые реализуют функцию сокрытия защищаемых информационных систем, а также дезинформируют потенциальных нарушителей. Сбор и фиксация данных о совершенных атаках на ИС, межсетевое экранирование, системы обнаружения вторжений и дезинформация потенциальных нарушителей – с их помощью ЛИС позволяют в реальном масштабе времени выявлять совершаемые атаки, направлять их на ложные объекты, исследовать действия нарушителей и определять их намерения, а также выявлять неизвестные ранее уязвимости ИС[2, 28].

Развитию практики применения ЛИС для защиты информационных систем способствует всѐ более активное внедрение технологий виртуализации, появление программных средств виртуализации, которые дают возможность сгенерировать виртуальную инфраструктуру и управлять ею. Перед использованием ЛИС необходимо рассчитать, насколько эффективно можно с еѐ помощью ввести в заблуждение нарушителя и при этом не создать высокой дополнительной вычислительной нагрузки для функционирования защищаемой информационной системы, так как при использовании технологий виртуализации ЛИС будет потреблять вычислительный ресурс истинной информационной системы. Однако

при использовании ложной информационной системы следует помнить о том, что чем больше ложных объектов создается, тем меньше вероятность нападения на реальный элемент информационной системы. Единственный недостаток данного подхода заключается в следующем: чем больше ложных объектов в системе, тем больше требуется ресурсов для ее создания. Также требуется квалифицированный и обученный персонал для обслуживания ЛИС [2, 28].

Следует отметить, что при применении такого подхода для защиты информации необходимы обязательный учет максимального числа возможных стратегий вероятного нарушителя, собственных стратегий стороны, защищающей информационную систему, а также точное понимание возникающих угроз и рисков при реализации каждой стратегии. То есть защищающая сторона должна принимать эффективные решения в условиях конфликтного взаимодействия с вероятным нарушителем. В то же время очевидно, что достижение заданной эффективности при принятии решений без обращения к конкретному математическому аппарату вызовет серьезные затруднения. Так как имеется изначальный конфликтный характер взаимодействия защищающей стороны и нарушителя, то целесообразно рассмотреть возможность использования аппарата теории игр[35].

Игра между защищающей стороной и нарушителем является игрой с неполной информацией, так как ни одной из сторон заранее неизвестен следующий ход другой стороны. Это является первой проблемой при использовании аппарата теории игр. Чтобы система защиты была эффективна, следует рассмотреть несколько игровых сценариев, по которым может идти игра между двумя сторонами, а именно: дуэль, игру с природой, задачу о садовнике [12].

Актуальность темы. В силу того, что поведение злоумышленника при реализации атаки в автоматизированной информационной системе редко имеет детерминированный характер, использование математического аппарата теории игр при принятии решений ложной информационной системой по стратегии защиты имеет огромную область исследования. Применимость теории игр в рамках работы ложной информационной системы мало исследована как в отечественных, так и зарубежных источниках. В связи с этим работа по оценке эффективности

разрабатываемых ложных информационных систем, использующих теорию игр при принятии стратегий защиты, является актуальной.

Объектом исследования дипломной работы является ложная информационная система, реализующая защиту автоматизированной информационной системы с использованием математического аппарата теории игр.

Предметом исследования дипломной работы является оценка эффективности работы ложной информационной системы с учетом игровых риск-моделей.

Цель дипломной работы заключается в разработке и формализация методик оценки рисков и управления эффективностью ложной информационной системы с учетом использования теоретико-игрового подхода. Для реализации данной цели необходимо решить приведенные ниже задачи:

1 провести исследование ЛИС с учетом оценки сценариев поведения злоумышленника;

2 сформулировать принципы риск-моделирования защиты автоматизированной информационной системы посредством ложной информационной системы

3 разработать математические модели атак, учитывающие этапность протекания процесса выбора стратегий защиты ложной информационной системы в рамках игровых риск-моделей;

4 разработать игровые сценарии взаимодействия ложной информационной системы и злоумышленника как в условиях неопределенности, так и в условиях риска;

5 провести оценку функции ущерба и рисков реализации атак в рамках применения различных игровых моделей взаимодействия ЛИС и злоумышленника;

6 разработать новый подход к управлению эффективностью ЛИС, основанный на оптимизации производительности, выделяемой для создания эмулированных объектов;

7 разработать алгоритм управления эффективностью ЛИС.

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 методытеории игр, методы теории вероятности, методы математической статистики и статистического анализа, методы теории графов, методы аналитического моделирования, методы теории рисков [16, 33, 34, 42].

Научная новизна исследования.

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

1 отличительной особенностью работы является изучение безопасности АИС сиспользованием теоретико-игрового подхода при принятии решений ЛИС;

2 в отличие от аналогичных работ, полученная риск-модель АИС, в отношении которой реализуются атаки,отличающаяся от известных введением учета различных игровых моделей и вероятностного подхода к принятию решений.

3 в данной работе получены функции эффективности работы ЛИС по различным риск-моделям, предложенуникальный подход к управлению эффективностью работы ЛИС, основанный на оптимизации производительности, выделяемой для создания эмулированных объектов.Разработанный алгоритм оптимизации позволяет перейти от качественных к количественным процедурам анализа эффективности и характеристик ЛИС.

Практическая ценность работы заключается в том, что:

1 анализ основных видов удаленных атак, воздействующих на компоненты АИС, позволяет выявить требования к увеличению эффективности, предъявляемые к разрабатываемым ЛИС;

2 построенная риск-модель АИС отражает этапы реализации защиты ЛИС и различные игровые сценарии, а так же позволяет всесторонне оценивать процесс реализации защиты. Вариативность сценариев выбора стратегий злоумышленника и ЛИС позволяет имитировать разнообразные варианты построения и функционирования ЛИС и, тем самым, оценивать эффективности работы ЛИС в составе различных АИС;

3 полученные выражения эффективности работы ЛИС на базе разработанных моделей реализации атаки позволяют не только оценить эффективность защиты, но и оптимизировать затраты на защиту АИС применительно к конкретным ЛИС.

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

projectIT

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

projectIT