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 всё большую актуальность и в Российской Федерации: Указ Президента №31с 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 «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.

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