

АНАЛИЗ МЕТОДИК ОПРЕДЕЛЕНИЯ НАДЕЖНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

Садикова А. А., Жарков А.Д. (Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», Санкт-Петербург)

Научный руководитель – Кузнецов А. Ю. (Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», Санкт-Петербург)

После создания системы защиты информации (СЗИ) на предприятии или ее проекта возникают вопросы оценки надежности СЗИ и времени преодоления системы защиты злоумышленником. Создание СЗИ осуществляется в три этапа. На первом этапе разрабатывается базовая модель системы, которая будет функционировать в компании. Второй этап включает разработку системы защиты. Третий, завершающий этап – это поддержка работоспособности системы, регулярный контроль и управление рисками. Важно, чтобы модуль защиты отличался гибкостью и позволял администратору безопасности быстро совершенствовать систему при обнаружении новых потенциальных угроз. При проектировании СЗИ необходимо учитывать, что защита информации должна быть постоянной, целевой, плановой (соответствует требованиям нормативно-правовых актов), активной, комплексной, универсальной (средства защиты информации выбираются в соответствии с обнаруженными утечками) и надежной.

Надежность системы защиты информации – характеристика способности программного, аппаратного, аппаратно-программного средства выполнить при определенных условиях требуемые функции в течение определенного периода времени.

Надежность является комплексным свойством, которое в зависимости от назначения объекта и условий его применения может включать безотказность, долговечность, ремонтпригодность и сохраняемость или определенные сочетания этих свойств.

Оценка надежности – определение численных значений показателей надежности объекта.

Для обработки информации, необходимость защиты которой определяется законодательством Российской Федерации или решением ее обладателя, должны создаваться автоматизированные системы в защищенном исполнении, в которых реализованы в соответствии с действующими нормативными правовыми актами требования о защите информации.

Существует устойчивое равновесие между объектами с низким уровнем безотказности, ремонт которых стоит дорого, и объектами с высоким уровнем безотказности, которые могут быть дорогими с точки зрения разработки и производства. Необходимо, чтобы эти характеристики были определены и конкретизированы.

Таким образом, целью работы является определение оптимальной для дальнейшего исследования методики определения надежности автоматизированной системы в защищенном исполнении.

В ходе работы были изучены и проанализированы методы оценки надежности автоматизированной системы в защищенном исполнении на примере следующих работ:

Варлатая С. К., Урзов А. Ю. Управление надежностью систем защиты информации как метод обеспечения защищенности информационных ресурсов,

Булгаков О. М., Удалов В. П., Кучмасов Е. А. Принципы построения модели надежности системы защиты информации,

Пономарев А.А. Оценка надежности систем защиты информации,

Щеглов А.Ю., Щеглов К.А. Математические модели и методы формального проектирования систем защиты информационных систем.

На основании анализа вышеперечисленных трудов в работе была выбрана методика оценки надежности автоматизированной системы в защищенном исполнении, на основании которой будет проведено дальнейшее исследование.

Садикова А. А.

Кузнецов А. Ю.