



8 (952) 106-88-60



vk.com/a.projectit



a.projectit

СОДЕРЖАНИЕ

projectIT

ВВЕДЕНИЕ

projectIT

projectIT

1. АНАЛИЗ УСЛОВИЙ ФУНКЦИОНИРОВАНИЯ СОВРЕМЕННЫХ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ

projectIT

1.1 Структура типовой ИВС. Структурная модель угроз информации в ИВС

projectIT

projectIT

1.2 Анализ современных подходов к защите ИВС

1.3 Анализ ЛИС, применяемых в современных ИВС. Характеристики, классификация и варианты применения



8 (952) 106-88-60



vk.com/a.projectit



a.projectit

1.3.1 История развития ЛИС и средств их создания

1.3.2 Анализ известных программных ЛИС

projectIT

1.3.3 Классификация ЛИС

projectIT

projectIT

1.3.4 Варианты применения современных ЛИС

1.4 Роль и место ЛИС в защите ИВС. Постановка задачи

Выводы по разделу

projectIT

2. РАЗРАБОТКА АЛГОРИТМОВ ЗАЩИТЫ

projectIT

projectIT

ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ МЕТОДАМИ ВВЕДЕНИЯ НАРУШИТЕЛЕЙ В ЗАБЛУЖДЕНИЕ

2.1 Методы введения нарушителей в заблуждение



8 (952) 106-88-60



vk.com/a.projectit



a.projectit

2.2 Алгоритмы функционирования ЛИС

2.2.1 Алгоритм эмуляции узлов ИВС

2.2.2 Алгоритм эмуляции прикладных систем

projectIT

2.2.3 Алгоритм эмуляции файловых ресурсов

projectIT

projectIT

2.3 Разработка требований к реализации базовых функций ЛИС

Выводы по разделу

ЗАКЛЮЧЕНИЕ

projectIT

Список использованных источников

projectIT

projectIT

projectIT

projectIT



8 (952) 106-88-60



vk.com/a.projectit



a.projectit

ВВЕДЕНИЕ

Необходимость обеспечения информационной безопасности требует поиска качественно новых подходов к решению многих технических и управленческих задач, связанных с использованием информационной сферы как совокупности информационных ресурсов и информационной инфраструктуры.

Всестороннее внедрение информационно-вычислительных систем (ИВС) общего назначения во все сферы деятельности субъектов хозяйствования предопределило появление неограниченного спектра угроз информационным ресурсам.

Несмотря на значительные результаты теоретических и прикладных исследований в области защиты информации в информационно-вычислительных системах, в частности криптографическими методами, резервированием, методами контроля межсетевого взаимодействия и т. п., недостаточно проработанной остается проблема защиты ИВС, подключенных к сетям связи общего пользования. В свою очередь технология ложных информационных систем является наиболее перспективной в этой области.

Учитывая, что во многих случаях объекты ИВС оснащаются разнотипными вычислительными средствами, существующие методы обеспечения информационной безопасности с помощью «защитных оболочек» не всегда эффективны и легко подвержены деструктивным воздействиям типа «отказ в обслуживании».

Решить проблему позволяет применение методов имитации ложных информационных объектов в защищаемых ИВС, заманивания в них нарушителей для отвлечения от реальных целей, т.е. введения нарушителей в заблуждение. На разработку таких методов защиты современных ИВС и реализацию их в виде алгоритмов функционирования ложных информационных систем и направлена эта работа.



8 (952) 106-88-60



vk.com/a.projectit



a.projectit

ЗАКЛЮЧЕНИЕ

В дипломном проекте была описана типовая структура вычислительной системы и структурная модель угроз информационным ресурсам информационно-вычислительных систем.

Проведен анализ современных подходов к защите информационно-вычислительных систем, который показывает, что большинство средств защиты направлены решение задачи управления доступом к информации. В то же время направление предупреждения угроз методами введения нарушителей в заблуждение не развиты.

Обширный анализ современных ложных информационных систем позволил выявить, что ложные информационные системы могли бы решать задачи защиты информационно-вычислительных систем методами введения в заблуждение, однако на сегодняшний день им, как правило, отводится роль приманок, применяемых в целях изучения возможностей злоумышленников.

Разработанный алгоритм функционирования ложной информационной системы и алгоритмы эмуляции ложной информационной системой узлов информационно-вычислительной системы, прикладных систем и файловых ресурсов, позволяют решать задачи введения противника в заблуждение и предупреждения таким образом несанкционированных воздействий на элементы информационно-вычислительной системы.

Экономическая эффективность применения предложенных технических решений обоснована.

Таким образом, поставленные на дипломное проектирование задачи выполнены, а цель дипломного проекта достигнута - разработаны алгоритмы защиты информационно-вычислительных систем методами введения нарушителей в заблуждение, применение которых позволяет снять ряд существенных противоречий в области защиты информации.