Т.М. Каннер

Программно-аппаратные средства защиты информации

Практикум

Москва
Типография «Вишневый пирог»
2025

УДК 004.056.5
ББК 30ф
К19

Каннер Т. М.
К19 Программно-аппаратные средства защиты информации: Практикум / Т.М. Каннер – М.: Типография «Вишневый пирог», 2025. – 318 с.

ISBN 978-5-6053673-9-0

Книга представляет собой практическое руководство по программно-аппаратным средствам защиты информации производства компании ОКБ САПР. В нем приводятся лабораторные работы по установке, настройке, применению и удалению аппаратного модуля доверенной загрузки, средств разграничения доступа для ОС Windows и Linux, защищенного служебного носителя данных, неперезаписываемого программно-аппаратного журнала событий безопасности, мобильного носителя лицензий, средства организации доверенного сеанса связи и персонального идентификатора пользователя.

Издание предназначено для студентов, обучающихся по специальностям высшего или среднего образования по УГПН 10.00.00 «Информационная безопасность» или другим смежным специальностям, а также слушателей курсов дополнительного профессионального образования по технической защите информации.

УДК 004.056.5
ББК 30ф

ISBN 978-5-6053673-9-0

Оглавление

ВВЕДЕНИЕ

Для каждого из нас жизнь немыслима без применения информационных технологий. Компьютеры обслуживают информационные системы различных отраслей нашей жизни: банковские, медицинские, транспортные, таможенные и многие другие. Однако, хранимая, обрабатываемая и передаваемая в данных системах информация может быть подвержена агрессивным воздействиям, в том числе и таким как – несанкционированный доступ. Поэтому, используя информационные технологии, крайне важно помнить о защите информации в них.

Согласно национальному стандарту ГОСТ Р 50922-2006 *защита информации* – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, а *средство защиты информации (СЗИ)* – это техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации [2].

Технические средства защиты информации – это устройства, которые обеспечивают безопасность информации при помощи аппаратных средств. Программные СЗИ защищают информацию, используя различные программы. Программно-технические средства защиты информации включают в свой состав программный и аппаратный компоненты, и поэтому в большинстве случаев называются «программно-аппаратными».

Данный практикум предназначен для изучения принципов работы, функциональных возможностей и практического применения программно-аппаратных СЗИ, а также освоения навыков их установки, настройки, применения и удаления.

Целью данного практикума является обучение установке, настройке, применению и удалению программно-аппаратных средств защиты информации производства компании ОКБ САПР.

В книге изучаются следующие программно-аппаратные комплексы (ПАК) средств защиты информации: СЗИ НСД «Аккорд-АМДЗ», ПАК СЗИ НСД «Аккорд-Win64», ПАК СЗИ НСД «Аккорд-X», ПАК «Секрет

особого назначения», ПАК «Программно-аппаратный журнал», ПАК «Мобильный носитель лицензий», СОДС «МАРШ!» и ПАК «ПИ ШИПКА». В соответствии с этим в практикуме выделены разделы, каждый из которых посвящен одному из указанных комплексов. В состав каждого раздела включены лабораторные работы по перечисленным программно-аппаратным комплексам, кроме ПАК СЗИ НСД «Аккорд-X». Для демонстрации возможностей ПАК СЗИ НСД «Аккорд-X» используется виртуальная машина с СПО «Аккорд-X К».

Перечень лабораторных работ следующий:

1. Установка аппаратной части и настройка учетных записей пользователей комплекса СЗИ НСД «Аккорд-АМДЗ».
2. Настройка и использование комплекса СЗИ НСД «Аккорд-АМДЗ».
3. Завершение работы с комплексом СЗИ НСД «Аккорд-АМДЗ».
4. Установка ПАК СЗИ НСД «Аккорд-Win64».
5. Учетные записи пользователей ПАК СЗИ НСД «Аккорд-Win64».
6. Права доступа пользователей ПАК СЗИ НСД «Аккорд-Win64».
7. Права доступа пользователей ПАК СЗИ НСД «Аккорд-Win64» (продолжение).
8. Контроль целостности объектов ПАК СЗИ НСД «Аккорд-Win64».
9. Дискреционный механизм управления доступом в ПАК СЗИ НСД «Аккорд-Win64».
10. Мандатный механизм управления доступом в ПАК СЗИ НСД «Аккорд-Win64».
11. Завершение работы с ПАК СЗИ НСД «Аккорд-Win64».
12. Установка СПО «Аккорд-X К».
13. Применение СПО «Аккорд-X К».
14. Удаление СПО «Аккорд-X К».
15. Установка, настройка и применение ПАК «Секрет особого назначения».
16. Установка, настройка и применение ПАК «Программно-аппаратный журнал».
17. Установка, настройка и применение ПАК «Мобильный носитель лицензий».

18. Установка, настройка и применение СОДС «МАРШ!».
19. Установка, настройка и применение ПАК «ПИ ШИПКА».

Лабораторные работы разделов выстроены в логической последовательности, позволяющей поэтапно осваивать возможности СЗИ (по конкретному ПАК). В связи с этим рекомендуется выполнять их в соответствии с очередностью. При этом каждая из работ содержит раздел «Подготовительные действия» с описанием действий, необходимых для выполнения выбранной работы при отклонении от определенной в практикуме последовательности.

Практикум может использоваться в процессе подготовки студентов, обучающихся по специальностям высшего или среднего образования по УГПН 10.00.00 «Информационная безопасность» или другим смежным специальностям, а также при обучении слушателей курсов дополнительного профессионального образования по технической защите информации.

В рамках дисциплины, которая реализуется с использованием практикума, выполнению каждой лабораторной работы должно предшествовать лекционное и/или семинарское занятие по данной теме. При этом в начале разделов каждого из рассматриваемых СЗИ есть теоретический материал, которого достаточно для освоения находящихся в нем лабораторных работ на должном уровне.

После некоторых лабораторных работ следуют задания для самостоятельного выполнения, рекомендуемые обучающимся в качестве домашних заданий при условии выдачи им программно-аппаратных комплексов в личное временное пользование.

В конце каждого раздела предлагаются контрольные вопросы по изученному СЗИ, которые можно использовать для проверки качества усвоения материала обучающимися и/или для их промежуточной аттестации.

В заключении приведен список тестовых вопросов по всему материалу практикума, которые можно использовать для проверки качества усвоения материала обучающимися и/или их итоговой аттестации.