Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»

А. А. Бабаева

ИНТЕГРИРОВАННЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ

Учебно-методическое пособие
по выполнению лабораторных работ
для студентов направления подготовки
10.05.03 Информационная безопасность автоматизированных систем

Калининград
Издательство ФГБОУ ВО «КГТУ»
2022

Рецензент
доцент кафедры информационной безопасности ФГБОУ ВО
«Калининградский государственный технический университет»
А.Г. Жестовский

Бабаева, А. А.
Интегрированные системы безопасности: учебно-методическое пособие по выполнению лабораторных работ для студентов направления подготовки 10.05.03 Информационная безопасность автоматизированных систем / А. А. Бабаева . – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2022. – 14 с.

Учебно-методическое пособие является руководством по изучению дисциплины «Интегрированные системы безопасности» студентами, которые обучаются по специальности 10.05.03 Информационная безопасность автоматизированных систем. Учебно-методическое пособие предназначено для приобретения практических навыков эксплуатации интегрированных систем безопасности в различных областях применения и изучения особенностей их использования.

Список лит. – 3 наименования.

Учебно-методическое пособие рассмотрено и одобрено в качестве локального электронного методического материала кафедрой информационной безопасности 19 мая 2022 г., протокол № 7

Учебно-методическое пособие по выполнению лабораторных работ рекомендовано к использованию в учебном процессе в качестве локального электронного методического материала методической комиссией института цифровых технологий ФГБОУ ВО «Калининградский государственный технический университет» 28 июня 2022 г., протокол № 4

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ

Данное учебно-методическое пособие предназначено для студентов направления подготовки 10.05.03 «Информационная безопасность автоматизированных систем», изучающих дисциплину «Интегрированные системы безопасности».

Цель лабораторного практикума по дисциплине: в результате освоения дисциплины ожидается, что студенты получат целостное представление особенностях проектирования и создания интегрированных систем безопасности, сформируют понятия о современных подходах к проектированию и построению, эксплуатации и модернизации систем безопасности на объектах.

Лабораторный практикум содержит 5 лабораторных работ.

В результате выполнения лабораторных работ у студентов должна сформироваться система знаний о теоретических, методических и технологических основах построения интегрированных систем безопасности объектов информатизации.

2. ЛАБОРАТОРНАЯ РАБОТА № 1. ОБЩИЕ ПРИНЦИПЫ ОРГАНИЗАЦИИ ЗАЩИТЫ ОБЬЕКТОВ ИНФОРМАТИЗАЦИИ

1. Общие сведения

Цель: Изучить принципы организации защиты информационных систем

Материалы, оборудование, программное обеспечение:

Для выполнения данной лабораторной работы потребуется персональный компьютер с установленным на нем офисным пакетом Microsoft Office и доступ в сеть Интернет.

Условия допуска к выполнению:

Подготовить конспект по теоретической части задания.

Критерии положительной оценки: предоставить преподавателю отчет (конспект с ответами на вопросы) в электронном виде.

Планируемое время выполнения:

Аудиторное время выполнения (под руководством преподавателя): 2 ч.

Время самостоятельной подготовки: 1 ч.

2. Теоретическое введение

Контрольные вопросы для самопроверки: не предусмотрены.

3. Задание к лабораторной работе

Ответить на список вопросов, приведенный ниже. Для этого самостоятельно найти нужную литературу (при необходимости) или проанализировать информацию, изученную ранее на других дисциплинах.

4. Методические указания и порядок выполнения работы

Ответить в электронном документе на следующие вопросы:

1. Определить объекты и субъекты защиты для типовой информационной системы.
2. Виды субъектов защиты и примеры их реального использования.
3. Указать основные принципы создания систем защиты.
4. Указать особенности применения систем защиты для объектов информатизации.
5. Требования к отчету и защите.

Подготовить отчет, разместить в ЭИОС и защитить у преподавателя.

Содержание отчета: титульный лист с указанием названия дисциплины, названия работы и фамилии студента, ответы на все вопросы из пункта 4.

3. ЛАБОРАТОРНАЯ РАБОТА № 2. КЛАССИФИКАЦИЯ НАРУШИТЕЛЕЙ И ПОТЕНЦИАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ

1. Общие сведения

Цель: способы определения актуальных угроз безопасности. Изучить классификацию нарушителей и определить актуальных нарушителей для типовой информационной системы.

Материалы, оборудование, программное обеспечение:

Для выполнения данной лабораторной работы потребуется персональный компьютер с установленным на нем офисным пакетом Microsoft Office и доступ в сеть Интернет.

Условия допуска к выполнению:

Успешное выполнение и защита лабораторной работы № 1.

Критерии положительной оценки: предоставить преподавателю отчет (конспект с ответами на вопросы) в электронном виде.

Планируемое время выполнения:

Аудиторное время выполнения (под руководством преподавателя): 2 ч.

Время самостоятельной подготовки: 1 ч.

2. Теоретическое введение

Контрольные вопросы для самопроверки: не предусмотрены.

3. Задание к лабораторной работе

Ответить на список вопросов, приведенный ниже. Для этого самостоятельно найти нужную литературу (при необходимости) или проанализировать информацию, изученную ранее на других дисциплинах.

4. Методические указания и порядок выполнения работы

Ответить в электронном документе на следующие вопросы:

- привести список уязвимостей и угроз для информационных систем;
- определить актуальные угрозы и ответить почему они такими являются;
- определить актуальных нарушителей и привести классификацию нарушителей;
- указать нормативные документы, на которые нужно опираться в этих вопросах.

5. Требования к отчету и защите

Подготовить отчет, разместить в ЭИОС и защитить у преподавателя.

Содержание отчета: титульный лист с указанием названия дисциплины, названия работы и фамилии студента, ответы на все вопросы из пункта 4.

4. ЛАБОРАТОРНАЯ РАБОТА № 3. ФИЗИЧЕСКАЯ ЗАЩИТА И ЗАЩИТА ОТ ВОЗДЕЙСТВИЯ ОКРУЖАЮЩЕЙ СРЕДЫ

1. Общие сведения

Цель: изучение важных аспектов управления ИБ организации, имеющих практическую направленность на управление физическим доступом к активам организации.

Материалы, оборудование, программное обеспечение:

Для выполнения данной лабораторной работы потребуется персональный компьютер с установленным на нем офисным пакетом Microsoft Office и доступ в сеть Интернет.

Условия допуска к выполнению:

Успешное выполнение и защита лабораторной работы № 2.

Критерии положительной оценки: предоставить преподавателю отчет (конспект с ответами на вопросы) в электронном виде.

Планируемое время выполнения:

Аудиторное время выполнения (под руководством преподавателя): 2 ч.

Время самостоятельной подготовки: 1 ч.

2. Теоретическое введение

Физическая защита предназначена для контроля и управления физическим доступом (КУД) к активам организации. Под доступом понимается перемещение людей (субъектов доступа), транспорта и других объектов (объектов доступа) в (из) помещения, здания, зоны и территории. КУД - комплекс мероприятий, направленных на предотвращения НСД - доступа субъектов или объектов, не имеющих права доступа1.

КУД обеспечиваются соответствующие средства контроля и управления доступом (средства КУД) - механические, электромеханические устройства и конструкции, электрические, электронные, электронные программируемые устройства, программные средства, обеспечивающие реализацию КУД. При этом средства управления - аппаратные средства (устройства) и программные средства, обеспечивающие установку режимов доступа, прием и обработку информации со считывателей, проведение идентификации и аутентификации, управление исполнительными и преграждающими устройствами, отображение и регистрацию информации. Совокупность средств КУД, обладающих технической, информационной, программной и эксплуатационной совместимостью, образуют систему контроля и управления доступом (СКУД).

При создании системы физической защиты (СФЗ) объекта решаются две важные задачи:

1) предотвращение несанкционированного проникновения нарушителя на объект с целью хищения или уничтожения активов организации;

2) защита объекта от воздействия стихийных сил и прежде всего, пожара и воды. Решение этих задач подразумевает учет большого количества различных факторов и направлено на сведение к минимуму возможностей несанкционированного проникновения на объект и к его жизненно важным центрам, вероятности осуществления актов промышленного шпионажа и последствий от воздействия стихии.

Хищение и саботаж на территории объекта могут быть предотвращены двумя способами: путем удержания нарушителей от совершения нежелательных действий или путем успешного противодействия нарушителям, для чего используются соответствующие методы обнаружения (раскрытие действий, совершаемых нарушителем), задержки (замедление продвижения нарушителя) и нейтрализации (сочетание ответных действий, останавливающих нарушителей перед тем, как они выполнят свою задачу), основанные на оценке текущей ситуации на объекте.

В основу создания СФЗ положены следующие общие принципы:

- непрерывность защиты, характеризующая постоянную готовность СФЗ к отражению угроз безопасности объекта;
- активность, предусматривающая прогнозирование действий нарушителей, разработку и реализацию опережающих мер по защите;
- скрытность, исключающая ознакомление посторонних лиц со средствами и процедурами защиты;
- целеустремленность, предполагающая сосредоточение усилий по предотвращению угроз наиболее ценным составляющим объекта;
- комплексное использование различных способов и средств защиты. В общем случае структура СФЗ объектов состоит из ряда подсистем.

Таким образом, основу СФЗ составляют механические средства и инженерные сооружения, препятствующие физическому движению нарушителей к месту нахождения объектов защиты, технические средства, информирующих сотрудников службы безопасности о проникновении нарушителя в контролируемую зону и позволяющие наблюдать обстановку в них, а также средства и люди, устраняющие угрозы. Использование при создании СФЗ современных технических средств охраны и средств обработки и представления информации привело к тому, что СФЗ превратились в автоматизированные интегрированные системы безопасности, комплексно выполняющие функций обеспечения безопасности объекта.

3. Задание к лабораторной работе

Ответить на список вопросов, приведенный ниже. Для этого самостоятельно найти нужную литературу (при необходимости) или проанализировать информацию, изученную ранее на других дисциплинах.

4. Методические указания и порядок выполнения работы

Ответить в электронном документе на следующие вопросы:

Как осуществляется физическая защита и защита от воздействия окружающей среды?

В чем разница понятий логического и физического доступа?

Как в организации создаются охраняемые зоны?

Что такое периметр безопасности?

Как защитить оборудование организации от различных видов угроз

5. Требования к отчету и защите

Подготовить отчет, разместить в ЭИОС и защитить у преподавателя.

Содержание отчета: титульный лист с указанием названия дисциплины, названия работы и фамилии студента, ответы на все вопросы из пункта 4.

5. ЛАБОРАТОРНАЯ РАБОТА №4. ПРОЕКТИРОВАНИЕ СИСТЕМ БЕЗОПАСНОСТИ

1. Общие сведения

Цель: Изучить основные способы проектирования систем безопасности, нормативные документы в этой области и создать проект типовой системы безопасности.

Материалы, оборудование, программное обеспечение:

Для выполнения данной лабораторной работы потребуется персональный компьютер с установленным на нем офисным пакетом Microsoft Office и доступ в сеть Интернет.

Условия допуска к выполнению:

Успешная защита лабораторной работы № 3.

Критерии положительной оценки: предоставить преподавателю отчет (конспект с ответами на вопросы) в электронном виде.

Планируемое время выполнения:

Аудиторное время выполнения (под руководством преподавателя): 2 ч.

Время самостоятельной подготовки: 1 ч.

2. Теоретическое введение

Контрольные вопросы для самопроверки: не предусмотрены.

3. Задание к лабораторной работе

Ответить на список вопросов, приведенный ниже. Для этого самостоятельно найти нужную литературу (при необходимости) или проанализировать информацию, изученную ранее на других дисциплинах.

4. Методические указания и порядок выполнения работы

Ответить в электронном документе на следующие вопросы:

- определить объекты и субъекты защиты для типовой информационной системы;
- виды субъектов защиты и примеры их реального использования;
- указать основные принципы создания систем защиты;
- указать особенности применения систем защиты для объектов информатизации.

5. Требования к отчету и защите

Подготовить отчет, разместить в ЭИОС и защитить у преподавателя.

Содержание отчета: титульный лист с указанием названия дисциплины, названия работы и фамилии студента, ответы на все вопросы из пункта 4.

6. ЛАБОРАТОРНАЯ РАБОТА № 5. ОЦЕНКА ЭФФЕКТИВНОСТИ СИСТЕМЫ БЕЗОПАСНОСТИ

1. Общие сведения

Цель: Изучить способы оценки эффективности систем безопасности и привести оценку самостоятельно

Материалы, оборудование, программное обеспечение:

Для выполнения данной лабораторной работы потребуется персональный компьютер с установленным на нем офисным пакетом Microsoft Office и доступ в сеть Интернет.

Условия допуска к выполнению:

Успешно выполненная лабораторная работа № 4.

Критерии положительной оценки: предоставить преподавателю отчет (конспект с ответами на вопросы) в электронном виде.

Планируемое время выполнения:

Аудиторное время выполнения (под руководством преподавателя): 2 ч.

Время самостоятельной подготовки: 1 ч.

2. Теоретическое введение

Контрольные вопросы для самопроверки: не предусмотрены.

3. Задание к лабораторной работе

Ответить на список вопросов, приведенный ниже. Для этого самостоятельно найти нужную литературу (при необходимости) или проанализировать информацию, изученную ранее на других дисциплинах.

4. Методические указания и порядок выполнения работы

Ответить в электронном документе на следующие вопросы:

- Привести основные способы оценки эффективности систем защиты объектов
- выбрать наиболее подходящий и объяснить причину своего выбора
- провести оценку эффективности для типового объекта

5. Требования к отчету и защите

Подготовить отчет, разместить в ЭИОС и защитить у преподавателя.

Содержание отчета: титульный лист с указанием названия дисциплины, названия работы и фамилии студента, ответы на все вопросы из пункта 4.

7. ЗАКЛЮЧЕНИЕ

Учебно-методическое пособие позволяет студентам освоить базовые знания и приобрести навыки по разработке, защите и эксплуатации интегрированных систем безопасности.

Для углубления своих знаний в области создания интегрированных систем безопасности и обеспечения их защищенности студенты могут использовать учебные ресурсы, часть из которых представлена в списке литературы.

8. ЛИТЕРАТУРА

1. Грибунин, В. А. Комплексная система защиты информации на предприятии: учебное пособие / В. А. Грибунин, В. В. Чудовский. – Москва: Академия, 2009.

2. Гришина, Н. В. Комплексная система защиты информации на предприятии на предприятии: учебное пособие / Н. В. Гришина. – Москва: ФОРУМ, 2011.

3. Гузаиров, М. Б. Технические средства защиты: учебное пособие / М. Б. Гузаиров. – Уфа: УГАТУ, 2007.

4. Михайлов, Ю. Б. Научно-методические основы обеспечения безопасности защищаемых 7 объектов / Ю. Б. Михайлов. – Москва: Горячая линия-Телеком, 2015.

Дополнительная литература:

1. Барсуков, В. С. Современные технологии безопасности / В. С. Барсуков, В. В. Водолазкий. – Москва: Нолидж, 2000.

2. Садердинов, А. А. Информационная безопасность предприятия: учебное пособие / А. А. Садердинов, В. А. Трайнёв, А. А. Федулов. – Москва: Дашков и Кº, 2006.

3. Синилов, В. Г. Системы охранной, пожарной и охранно-пожарной сигнализации: учебник / В. Г. Синилов. – Москва: ИРПО: Академия, 2003. 4. ГОСТ Р 53704-2009 Системы безопасности комплексные и интегрированные. Общие технические требования. – Москва: Стандартинформ, 2010.

Локальный электронный методический материал

Алина Андреевна Бабаева

ИНТЕГРИРОВАННЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ

Редактор Г. А. Смирнова

Уч.-изд. л. 0,9. Печ. л. 0,9

Издательство федерального государственного бюджетного
образовательного учреждения высшего образования
«Калининградский государственный технический университет».
236022, Калининград, Советский проспект, 1