МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«__8__» ___08___ 2023 г.

Технологии обеспечения информационной безопасности объектов

Методические указания по организации самостоятельной работы по дисциплине «Технологии обеспечения информационной безопасности объектов» для студентов направления подготовки 10.04.01 «Информационная безопасность»

Курск 2023

УДК 004.773.5

Составители: Кулешова Е.А.

Рецензент

Кандидат технических наук, доцент кафедры
вычислительной техники А.В. Киселев

Технологии обеспечения информационной безопасности объектов: методические указания для самостоятельной работы / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 8 с.: Библиогр.: с. 8.

Содержат сведения по вопросам самостоятельной работы на протяжении изучения дисциплины. Указывается порядок выполнения самостоятельных работ, содержание работ.

Предназначены для студентов направления подготовки 10.04.01 «Информационная безопасность».

Текст печатается в авторской редакции
Подписано в печать . Формат 60x84 1/16.
Усл. печ.л. . Уч. –изд.л. .Тираж 50 экз. Заказ .
Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Содержание самостоятельной работы

	Тема СРС	Задание
1	Понятия и определения технических средств охраны. Структура автоматизированной системы охраны	1. Составьте список основных технических средств охраны и определите их функциональные характеристики, например, видеонаблюдение, сигнализация, контроль доступа и т.д. 2. Рассмотрите принципы работы и особенности каждого из технических средств охраны и объясните их значение для обеспечения безопасности объектов. 3. Сравните различные модели и производителей технических средств охраны и оцените их преимущества и недостатки. 4. Изучите основные компоненты структуры автоматизированной системы охраны, такие как датчики, исполнительные устройства, центральные элементы управления и т.д. 5. Разработайте диаграмму, иллюстрирующую взаимодействие между компонентами системы охраны и объясните их роль в обеспечении безопасности объектов. 6. Исследуйте принципы работы сетевых коммуникаций и интеграцию автоматизированных систем охраны с другими системами (например, пожарной сигнализацией или системами контроля доступа).
2	Варианты программно-аппаратной реализации ТСО	1. Изучите различные варианты программной и аппаратной реализации технических средств охраны, такие как выбор оборудования, установка и настройка программного обеспечения и т.д. 2. Разработайте инструкцию или схему по установке и настройке конкретного технического средства охраны (например, системы видеонаблюдения или сигнализации). 3. Оцените процесс интеграции различных технических средств охраны и опишите возможные проблемы, с которыми может столкнуться охранная система.
3	Методология разработки концепции комплексного обеспечения безопасности объектов	1. Исследуйте различные методологии разработки концепции комплексного обеспечения безопасности объектов охраны, такие как системный анализ, SWOT-анализ или методология разработки информационных систем. 2. Разработайте методологию, позволяющую оценить требования безопасности конкретного

	охраны	объекта и определить необходимые технические средства и меры безопасности. 3. Примените разработанную методологию к конкретному объекту охраны, проведите анализ и предложите рекомендации по улучшению системы безопасности.
4	Общий подход к категорированию объектов охраны	Изучите общий подход к категоризации объектов охраны на основе их критичности и специфики (например, банки, аэропорты, промышленные объекты и т.д.).
5	Классификация нарушителей информационной безопасности, угроз ИБ и технических средств охраны	1. Проанализируйте реальные случаи нарушений безопасности и определите, какие классификации нарушителей они соответствуют, а также предложите соответствующие меры для их предотвращения и обнаружения. 2. Выберите три различных типа объектов охраны, например, банк, аэропорт и офисный здание. 1. Для каждого объекта охраны проведите анализ и определите следующие характеристики: o Описание объекта (цель использования, физические параметры и т.д.). o Уровень критичности объекта (высокий, средний, низкий). o Существующие угрозы безопасности, связанные с объектом. o Возможные последствия нарушения безопасности. o Существующие меры безопасности и технические средства охраны. 2. Классифицируйте каждый объект охраны, опираясь на его уровень критичности и тип угроз. 3. Разработайте общий подход к категорированию объектов охраны, учитывая их классификацию и важность. 4. Обоснуйте предложенный подход и объясните, как он может быть применен для определения необходимого уровня безопасности и выбора соответствующих технических средств охраны для каждого объекта.

КОНТРОЛЬНЫЕ ВОПРОСЫ

Тема №1 «Понятия и определения технических средств охраны. Структура автоматизированной системы охраны»

1. Что такое технические средства охраны (ТСО)?
2. Назначение и цели ТСО.
3. Основные виды ТСО.
4. Дайте определение термину «Техническая безопасность».
5. Дайте определение термину «Компьютерная безопасность».
6. Что такое канал сигнализации? Как можно классифицировать ССОИ.
7. Что подразумевается под техническими средствами охраны?
8. Какие основные виды технических средств охраны существуют?
9. Какие функции выполняют технические средства охраны?
10. Какова структура автоматизированной системы охраны?

Тема №2 «Варианты программно-аппаратной реализации ТСО»

1. Что такое диалог человека и КТСО и для чего он нужен?
2. Нарисуйте структурную схему, поясняющую принцип контроля состояния СО и объясните её.
3. Каким образом можно представить схему функционирования ССОИ?
4. Перечислите и охарактеризуйте методы отображения информации, применяемые в ССОИ.
5. Как можно организовать информационный обмен ССОИ с подсистемами КТСО или с другими самостоятельными системами специальной защиты?
6. Какие программные средства используются для реализации технических средств охраны?
7. Какая роль аппаратного обеспечения в программно-аппаратной реализации ТСО?
8. Какие типы датчиков могут быть использованы в программно-аппаратной реализации ТСО?
9. Каким образом программно-аппаратная реализация ТСО может быть интегрирована с системой видеонаблюдения?
10. Какие возможности предоставляют программно-аппаратные комплексы для обработки и анализа данных, получаемых от технических средств охраны?

Тема №3 «Методология разработки концепции комплексного обеспечения безопасности объектов охраны»

1. Перечислите укрупненные признаки, по которым принято классифицировать ССОИ.

2. Что такое ТСО, каковы основные подходы к их классификации? Приведите пример их классификации.

3. Что такое ЧЭ, каковы основные подходы к их классификации? Приведите пример и классификации.

4. Перечислите виды ССОИ в зависимости от структурной схемы построения.

5. Перечислите виды ССОИ в зависимости от способа подключения средства обнаружения (СО).

6. Какой признак классификации характеризует степень безопасности канала сигнализации? Перечислите виды ССОИ в зависимости от этого признака.

7. Какие основные шаги включает методология разработки концепции комплексного обеспечения безопасности объектов охраны?

8. Какие аспекты учитываются при определении требований к комплексному обеспечению безопасности объектов охраны?

9. Какой подход используется при анализе и выборе технических средств охраны в рамках разработки концепции комплексного обеспечения безопасности?

10. Как осуществляется оценка эффективности разработанной концепции комплексного обеспечения безопасности объектов охраны?

Тема №4 «Общий подход к категорированию объектов охраны»

1. Назовите категории объектов охраны.

2. Каковы факторы внешней среды, влияющие на выбор тактико-технических характеристик СО?

3. Как разделяются ССОИ по способам обеспечения контроля работоспособности аппаратуры?

4. Перечислите основные функции, выполняемые ССОИ в составе комплексов ТСО.

5. Как разделяются ССОИ по возможности хранения и документирования (распечатки) оперативной информации?

6. Что подразумевается под категорированием объектов охраны?

7. Какие основные критерии используются при категорировании объектов охраны?

8. Какие типы угроз обычно учитываются при определении категории объекта охраны?

9. Какие меры безопасности могут быть рекомендованы для каждой категории объектов охраны?

10. Какова роль и ответственность службы охраны при категорировании объектов охраны?

Тема №5 «Классификация нарушителей информационной безопасности, угроз ИБ и технических средств охраны»

1. Что такое "модель" нарушителя, какие типы "моделей" нарушителей рассматриваются?

2. Назовите типы моделей нарушителей, сформулируйте их отличительные признаки.

3. Нарисуйте и прокомментируйте структурную схему передачи информации о наличии нарушителя.

4. Назовите типы ССОИ в зависимости от их устойчивости к обходу, сформулируйте их отличительные признаки.

5. Решение каких задач предполагает "Системная концепция обеспечения комплексной безопасности?

6. Расскажите о классификации нарушителей, исходя из их "моделей" и способов реализации угроз безопасности.

7. Как осуществляется классификация нарушителей информационной безопасности?

8. Какие типы угроз информационной безопасности обычно выделяются при классификации?

9. Какие факторы учитываются при выборе и использовании технических средств охраны?

10. Какие основные категории технических средств охраны существуют и в каких случаях они применяются?

ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННЫХ РЕСУРСОВ

1. Технологии обеспечения безопасности информационных систем : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. - URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.

2. Основы администрирования информационных систем : учебное пособие / Д. О. Бобынцев, А. Л. Марухленко, Л. О. Марухленко [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 201 с. - URL: https://biblioclub.ru/index.php?page=book&id=598955 (дата обращения: 22.05.2023). - Режим доступа: по подписке. - Текст : электронный.

3. Горбунов, А. В. Проектирование защищённых оптических телекоммуникационных систем : учебное пособие / А. В. Горбунов, Ю. В. Зачиняев, А. П. Плёнкин. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2019. – 128 с. - URL: https://biblioclub.ru/index.php?page=book&id=598665 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.

4. Ищейнов, В. Я. Информационная безопасность и защита информации : теория и практика : учебное пособие / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. - URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.

5. Аверченков, В. И. Служба защиты информации : организация и управление : учебное пособие / В. И. Аверченков, М. Ю. Рытов. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 186 с. – URL: https://biblioclub.ru/index.php?page=book&id=93356 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.