МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра информационной безопасности

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.03.01 Информационная безопасность

Код и наименование направления подготовки/специальности

«Организация и технология защиты информации
(по отрасли или в сфере профессиональной деятельности)»

Наименование направленности (профиля)/ специализации

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2023

СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ
Рабочая программа дисциплины

Составитель:
д.т.н, профессор В.В. Арутюнов

Ответственный редактор
к.и.н., доцент, заведующая кафедрой ИБ Г.А. Шевцова

УТВЕРЖДЕНО
Протокол заседания кафедры
Информационной безопасности
№ 9 от 17.03.2023

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Целью дисциплины:формирование у студентов знаний по системам контроля и управления доступом, инженерно-техническим средствам охраны (СКУД и ИТСО) и формирование навыков работы по их использованию в системе защиты объекта от физического доступа посторонних лиц.

Задачи дисциплины: изучение факторов, влияющих на защиту объекта от физического несанкционированного доступа; определение категории объекта защиты; анализ принципов и основных требований по обеспечению безопасности объекта защиты; разработка технических решений и порядка проведения работ по оборудованию объекта защиты СКУД и ИТСО.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК-6 Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-6.1 Знает оценки работоспособности применяемых средств защиты информации с использованием штатных средств и методик	Знать: принципы работы программных средств системного, прикладного и специального назначения, инструментальных средств.
	ПК-6.2 Умеет оценить эффективности применяемых средств защиты информации с использованием штатных средств и методик	Уметь: выбирать, устанавливать и настраивать средства системного, прикладного и специального назначения.
	ПК-6.3 Владеет навыками определения уровня защищенности и доверия средств защиты информации	Владеть: навыками настройки и эксплуатации инструментальные средства, языки и системы программирования для решения профессиональных задач с соблюдением требований по защите информации.
ПК-3 Способен администрировать подсистемы информационной безопасности объекта защиты	ПК-3.1 Знает требования к встроенным средствам защиты информации программного обеспечения	Знать: основные методы управления защитой информации, информационные ресурсы и базовой модели нарушителя ФСТЭК России
	ПК-3.2 Умеет анализировать угрозы безопасности информации программного обеспечения, формулировать и обосновывать правила безопасной эксплуатации программного обеспечения, производить проверку соответствия реальных характеристик программно-аппаратных средств защиты информации заявленным в их технической документации	Уметь: классифицировать угрозы, разрабатывать технические предложения по совершенствованию системы управления защиты информации автоматизированных систем, проводить аудит с целью оценки рисков

	ПК-3.3 Владеет навыками ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования	Владеть: навыками по разработке организационно-технических по защите информации, приемы и принципы в соответствие с ЕСКД, ЕСПД и другими нормативно-правовыми документами

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Системы контроля и управления доступом» относится к части, формируемой участниками образовательных отношений, блока дисциплин учебного плана.
Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Электроника и схемотехника», «Аппаратные средства вычислительной техники», «Операционные системы».
В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Комплексная защита объектов информатизации», «Безопасность вычислительных сетей», «Безопасность систем баз данных».

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет _3з.е., 108 академическихчаса.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
5	Лекции	**24**
5	Практические работы	**36**
Всего:		**60**

Объем дисциплины в форме самостоятельной работы обучающихся составляет _30_ академических часа.

3. Содержание дисциплины

Тема 1. Методы и средства технической разведки

Деятельность государств по добыванию с помощью технических средств добывать сведения. Устройства и технологии, позволяющие получать сведения технического характера. Принципы организации и ведения технической разведки. Классификация технической разведки. Способы перехвата.

Тема 2. Первоочередные мероприятия по обеспечению информационной безопасности и контроль эффективности системы защиты, и рассмотрение требований к защите информации.

Определение объектов защиты. Классификация объектов защиты. Система мер, рекомендуемая для большинства компаний. Организационные меры. Установка градации сотрудников и их уровней доступа к информации. Обеспечение технической защиты помещений и оборудования с дальнейшей сертификацией классов защиты. Обеспечение защиты информации при управлении доступом. Предотвращение утечек информации. Управление инцидентами информационной безопасности.Требования к защите информации.

Тема 3. Методы контроля эффективности мер защиты информации в автоматизированных система

Проверка соответствия. Оценка возможностей. Анализ разрешенных и запрещенных связей. Проведение оценки соответствия. Требования к средствам контроля защищенности информации. Автоматизированный контроль. Система контроля. Документирование результатов контроля.

Тема 4. Средства оперативного контроля и регистрации событий безопасности

Средства разграничения и контроля целостности. Средства объективного контроля.оперативного ознакомления администратора безопасности. Подключение к файловому серверу. Запуск и завершение программы. Измерение. Регистрация.Получение первичной информации.

Тема 5. Средства контроля эффективности мер защиты от утечки по техническим каналам

Технические мероприятия. Активные технические средства защиты информации. Пассивные технические средства защиты информации. Контроль и ограничение доступа к ИС и в выделенные помещения с помощью технических средств и систем. Экранирование ОТСС и их соединительных линий. Установка специальных средств защиты в ВТСС, обладающих "микрофонным эффектом" и имеющих выход за пределы контролируемой зоны. Установка специальных диэлектрических вставок в оплетки кабелей электропитания, труб систем отопления, водоснабжения и канализации, имеющих выход за пределы контролируемой зоны. Установка в цепях электропитания ОТСС, а также в линиях осветительной и розеточной сетей выделенных помещений помехоподавляющих фильтров.

Тема 6. Проектирование системы защиты от НСД

Классификация мер и средств защиты. Меры по идентификации и аутентификации. Общие сведения о проектировании СЗИ. Стадии проектирования и основные подходы к встраиванию СЗИ. Принципы и методы построения защищённых АС. Место и роль спецификации при проектировании СЗИ. Разработка технического проекта. Разработка рабочей документации. Подготовка и оформление технической документации. Разработка порядка сопровождения. Разработка порядка и этапов внедрения СЗИ.

Тема 7.Аттестация автоматизированной системы по требованиям безопасности

ПАК "Сигурд".Назначение и состав. Программная оболочка. Достоинства и недостатки. Основные технические характеристики. Мероприятия по выявлению технических каналов утечки информации. Оценка защищенности информации от утечки. Принцип проведения исследований. Отличительные особенности от других систем. Действия персонала при проведении исследований. Оценка результатов.

4. Образовательные технологии

№ п/п	**Наименование раздела**	**Виды учебных занятий**	**Образовательные технологии**
1	**2**	**3**	**4**
1.	Общая характеристика процесса проектирования защищенных автоматизированных систем	Лекция 1. Самостоятельная работа	Традиционная лекция с использованием презентаций Опрос, тест Подготовка к занятиям с использованием ЭБС
2	Исходные данные для проектирования.	Лекция 2.	Традиционная лекция с использованием презентаций

		Практическое занятие 1. Самостоятельная работа	Занятия с использованием специализированного ПО Опрос, тест Подготовка к занятиям с использованием ЭБС
3	Организационные процессы создания автоматизированных систем	Лекция 3. Практическое занятие 2. Самостоятельная работа	Традиционная лекция с использованием презентаций Занятия с использованием специализированного ПО Опрос, тест Подготовка к занятиям с использованием ЭБС
4	Модели жизненного цикла автоматизированных систем	Лекция 4. Практическое занятие 3. Самостоятельная работа	Традиционная лекция с использованием презентаций Занятия с использованием специализированного ПО Опрос, тест Подготовка к занятиям с использованием ЭБС
5	Особенности проектирования комплексной системы информационной безопасности	Лекция 5. Практическое занятие 4. Самостоятельная работа	Традиционная лекция с использованием презентаций Занятия с использованием специализированного ПО Опрос, тест Подготовка к занятиям с использованием ЭБС
6	Проектирование системы защиты от НСД	Лекция 6. Практическое занятие 5. Самостоятельная работа	Традиционная лекция с использованием презентаций Занятия с использованием специализированного ПО Опрос, тест Подготовка к занятиям с использованием ЭБС
7	Аттестация автоматизированной системы по требованиям безопасности	Лекция 7. Практическое занятие 6. Самостоятельная работа	Традиционная лекция с использованием презентаций Опрос, тест Занятия с использованием специализированного ПО Подготовка к занятиям с использовани-

			ем ЭБС

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции**;**

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль:		
– опрос (темы 1-3)	*4 балла*	*12 баллов*
– тест (темы 4-7)	*3 балла*	*12 баллов*
– практическоезанятие(темы 1-6)	*6 баллов*	*36 баллов*
Промежуточная аттестация – экзамен с оценкой (вопросы по билетам)		*40 баллов*
Итого за семестр		100 баллов

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (EuropeanCreditTransferSystem; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 –67	удовлетворительно		D
50 –55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	зачтено	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	зачтено	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	зачтено	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Устный опрос

Устный опрос – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объёма знаний, обучающегося по определённому разделу, теме, проблеме и т.п.

Примерные вопросы к опросу – *проверка сформированности компетенций – ПК-6; ПК-3*

1. Понятие контрольно-пропускного режима.
2. Разработка инструкции о пропускном режиме.
3. Оборудование пропускных пунктов.
4. Основные требования к СКУД.
5. Классификация СКУД.
6. Основные виды СКУД.
7. Базовые компоненты контроллеров СКУД.
8. Основные характеристики СКУД.
9. Понятие идентификатора пользователя.
10. Основные функции СКУД.
11. Особенности распределённой структуры СКУД.
12. Основные типы устройств идентификации.
13. Особенности программного обеспечения для крупных СКУД.
14. Основные этапы биометрической технологии идентификации личности.
15. Особенности автономных СКУД.
16. Выбор биометрических СКУД.

Примерная тематикаконтрольных работ – *проверка сформированности компетенций – ПК-6; ПК-3*

1. Схема разветвлённой сети СКУД.
2. Цели создания контрольно-пропускного режима.
3. Подготовка исходных данных для организации контрольно-пропускного режима.
4. Основные задачи создания контрольно-пропускного режима.
5. Базовые требования к системам контроля управления доступом.
6. Основные этапы подготовки исходных данных для организации контрольно-пропускного режима.
7. Характеристика кодонаборных устройств.
8. Основные методы биометрического контроля.
9. Классификация турникетов в СКУД.
10. Особенности идентификация по радужной оболочке глаз.
11. Характеристика сетевых контроллеров.
12. Базовые методы биометрического контроля.
13. Распределенные системы контроля и управления доступом.
14. Особенности сетевых систем контроля и управления доступом
15. Общие вопросы выбора СКУД.
16. Особенности выбора СКУД по техническим показателям.

Примерная тематика вопросов для экамена – *проверка сформированности компетенций – ПК-6; ПК-3*

1. Цели и задачи создания контрольно-пропускного режима.
2. Классификация систем контроля и управления доступом (СКУД).
3. Состав СКУД.
4. Особенности СКУД для крупных распределенных объектов.
5. Основные средства идентификации и аутентификации.
6. Классификация биометрических средств идентификации личности.
7. Основные характеристики биометрических средств идентификации личности.
8. Базовые методы биометрического контроля.
9. Особенности реализации статических методов биометрического контроля.
10. Особенности идентификация по радужной оболочке глаз.
11. Классификация турникетов в СКУД.
12. Базовые типы шлюзовых кабин.
13. Особенности сетевых контроллеров СКУД.
14. Распределенные системы контроля и управления доступом.
15. Сетевые системы контроля и управления доступом.
16. Биометрические системы контроля и управления доступом.
17. Особенностиинтегрированных СКУД.
18. Основные рекомендации по выбору средств и систем контроля доступа.
19. Особенности выбора СКУД по техническим показателям.
20. Особенности выбора биометрических СКУД.

Примерные тестовые задания
- проверка сформированности компетенций – ПК-6; ПК-3

1. Перечень сведений, доступ к которым не может быть ограничен определен:
а) Федеральным законом от 27 июля 2006 г. N 149-ФЗ;
б) Указом Президента РФ от 6 марта 1997 г. No 188;
в) Указом Президента РФ от 30 ноября 1995 г. N 1203.
2. Что такое доктрина информационной безопасности РФ
а) совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации;
б) совокупность нормативных актов, обязательных для выполнения всеми хозяйствующими субъектами.
в) совокупность документов, регламентирующих организационно-технические мероприятия по обеспечению информационной безопасности Российской Федерации.
3. В российской практике проектирование ведётся ...
a. Поэтапно в соответствии со стадиями, регламентированными ГОСТ 2.103-68.
b. в соответствии со стадиями, регламентированными ГОСТ 2.103-98.
c. поэтапно в соответствии со стадиями, регламентированными ГОСТ 2.103-78.
d. поэтапно в соответствии со стадиями, регламентированными ГОСТ 2.103-98.
4. Действия, направленные на устранение действующей угрозы и конкретных преступных действий относятся к:
а) предупреждению угроз;
б) выявлению угроз;
в) локализации угроз;
г) ликвидации последствий угроз.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Литература
Основная

1. *Олифер В.Г.* Компьютерные сети : принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. – 3-е изд. – М. [и др.] : Питер, 2008. – 957 с.
2. *Митюшин Д.А.* Использование программного комплекса CiscoPacketTracer v.7.3 в изучении сетевых технологий: учебно-практическое пособие (практикум) / Д. А. Митюшин ; Российский государственный гуманитарный университет. – М.: Изд-во РГГУ, 2021. – 217 с.
3. Голиков А. М. Основы проектирования защищенных телекоммуникационных систем: учебное пособие, Томск: ТУСУР, 2016. –396 с., http://biblioclub.ru
4. Поликанин, А. Н. Технические средства охраны и видеонаблюдения. Системы видеонаблюдения и тепловизионного контроля : учебное пособие / А. Н. Поликанин. — Новосибирск :СГУГиТ, 2021. — 46 с. — ISBN 978-5-907320-92-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/222380 (дата обращения: 01.04.2023). — Режим доступа: для авториз. пользователей.

Дополнительная

1. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/
2. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. http://rkn.gov.ru/Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.
2. Nginx.org – [Электронный ресурс] : Режим доступа : https://nginx.org/ru, свободный. – Загл. с экрана
3. WiresharkDeveloper’sGuide [Электронный ресурс]: Режим доступа: https://www.wireshark.org/docs/wsdg_html_chunked/, свободный. – Загл. с экрана

Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru
Электронная библиотека Grebennikon.ruwww.grebennikon.ru

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения:

1) для лекционных занятий - учебная аудитория, доска, компьютер или ноутбук, проектор (стационарный или переносной) для демонстрации учебных материалов.

Состав программного обеспечения:
1. Windows
2. MicrosoftOffice
3. KasperskyEndpointSecurity

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

2) для практических занятий – компьютерный класс или лаборатория, доска, проектор (стационарный или переносной), компьютер или ноутбук для преподавателя, компьютеры для обучающихся.

Состав программного обеспечения:
1. Windows
2. MicrosoftOffice
3. KasperskyEndpointSecurity
4. Mozilla Firefox
5. Cisco Packet Tracer v.7.2

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительныеметоды обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата:лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением;экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут

использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.
- для глухих и слабослышащих: в печатной форме, в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:устройством для сканирования и чтения с камерой SARA CE;дисплеем Брайля PAC Mate 20;принтером Брайля EmBrailleViewPlus;
- для глухих и слабослышащих:автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата:передвижными, регулируемыми эргономическими партами СИ-1;компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1 Планы практических занятий

Темы учебной дисциплины предусматривают проведение практических занятий, которые служат как целям текущего и промежуточного контроля подготовки студентов, так и целям получения практических навыков применения методов выработки решений, закрепления изученного материала, развития умений, приобретения опыта решения конкретных проблем, ведения дискуссий, аргументации и защиты выбранного решения. Помощь в этом оказывают задания для практических занятий, выдаваемые преподавателем на каждом занятии.

Цельюпрактических занятий является закрепление теоретического материала и приобретение практических навыков работы с соответствующим оборудованием, программным обеспечением и нормативными правовыми документами.

Тематикапрактических занятий соответствует программе дисциплины.

Практическая работа № 1 (6 ч)*Определение целей защиты информации на предприятии регионального уровня. Рассмотрение особенностей объекта защиты информации–ПК-6; ПК-3*

Задания:

1. Осуществить принятие решения о необходимости защиты информации, содержащейсяв информационной системе.
2. Определить угрозы безопасности информации, реализация которыхможет привести к нарушению безопасности информации в информационной системе.
3. Определить требования к системе защиты информации информационной системы.

Практическая работа № 2 (6 ч)*Определение каналов утечки информации и выработка мер защиты –ПК-6; ПК-3*

Задания:

1. Рассмотрение схемы технического канала утечки информации.

2. Анализ активного метода защиты информации от утечки.
3. Анализ пассивного метода от утечки инормации.

Практические работы № 3 (6 ч)*Порядок проведения контроля эффективности мер защиты инструментальным методом от НСД –ПК-6; ПК-3*
Задания:
1. Подготовка исходных данных.
2. Оценить эффективность мер защиты информации инструментальным методом.
3. Сделать выводы

Практическая работа № 4 (6 ч) ***Тестирование мер защиты на примере эшелонированной защиты от НСД–ПК-6; ПК-3***
Задания:
1. Подготовка исходных данных.
2. Оценить эффективность мер защиты информации инструментально-расчетным методом.
3. Сделать выводы

Практическая работа № 5 (6 ч)*Проведение контроля защищенности информации на объекте ВТ от утечки по каналу ПЭМИН –ПК-6; ПК-3*
Задания:
1. Изучение инструкции по эксплуатации.
2. Изучение схемы для определения побочных электромагнитных излучений информативного сигнала от технических средств и линий передачи информации.

Практическая работа № 6 (6 ч)*Аттестация автоматизированной системы по требованиям безопасности –ПК-6; ПК-3*
Задания:
1. изучить план-схему местности, границы контролируемой зоны объекта
2. определить реальные размеры зоны R2 технических средств, установленных на объекте, по соответствующим методикам из сборника методик инструментального контроля.

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина реализуется«Системы контроля и управления доступом» на факультете Информационных систем и безопасности кафедрой информационной безопасности.

Целью дисциплины: формирование у студентов знаний по системам контроля и управления доступом, инженерно-техническим средствам охраны (СКУД и ИТСО) и формирование навыков работы по их использованию в системе защиты объекта от физического доступа посторонних лиц.
Задачи дисциплины: изучение факторов, влияющих на защиту объекта от физического несанкционированного доступа; определение категории объекта защиты; анализ принципов и основных требований по обеспечению безопасности объекта защиты; разработка технических решений и порядка проведения работ по оборудованию объекта защиты СКУД и ИТСО.

Дисциплина направлена на формирование следующих компетенций:

ПК-3 – Способен администрировать подсистемы информационной безопасности объекта защиты.

ПК-6 – Способен принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

В результате освоения дисциплины (модуля) обучающийся должен:

Знать:

основные положения теории информационной безопасности и практики защиты информации от несанкционированного доступа;

нормативные правовые документы в области защиты информации;

математические модели безопасности и формальные модели доступа систем;

модели и методы защиты операционных систем;

принципы работы программных средств системного, прикладного и специального назначения, инструментальных средств;

основные проектные решения, средства и методы защиты информации от несанкционированного доступа.

Уметь:

решать типовые задачи с помощью методов защиты информации от несанкционированного доступа;

применять современные методы и методики защиты программ от программных средств скрытого информационного воздействия;

выбирать, устанавливать и настраивать средства системного, прикладного и специального назначения; применять современные методы и методики защиты программ от несанкционированного исследования, копирования, распространения и использования.

Владеть: методами разработки и использования средств защиты ПО;

навыками настройки и эксплуатации инструментальные средства, языки и системы программирования для решения профессиональных задач;

навыками эксплуатации защищенных программных средств, получивших широкое применение в современных автоматизированных системах.

По дисциплине предусмотрена промежуточная аттестация в форме экзамена.
Общая трудоёмкость освоения дисциплины составляет 3 зачётные единицы.