МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ

"БРАТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"

УТВЕРЖДАЮ

Проректор по учебной работе

_____Е.И.Луковникова

13 мая 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.04.ДВ.02.01 Комплексное обеспечение безопасности объекта информатизации

Закреплена за кафедрой **Информатики, математики и физики**

Учебный план b010302_24_ИПОиЗИ.plx
Направление: 01.03.02 Прикладная математика и информатика

Квалификация **Бакалавр**

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Виды контроля в семестрах:
Зачет 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	17			
Вид занятий	УП	РП	УП	РП
Лекции	17	17	17	17
Лабораторные	34	34	34	34
В том числе инт.	12	12	12	12
В том числе в форме практ.подготовки	34	34	34	34
Итого ауд.	51	51	51	51
Контактная работа	51	51	51	51
Сам. работа	57	57	57	57
Итого	108	108	108	108

Программу составил(и):
к.т.н., доц., Фигура К.Н. _____
Рабочая программа дисциплины

Комплексное обеспечение безопасности объекта информатизации

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 01.03.02 Прикладная математика и информатика (приказ Минобрнауки России от 10.01.2018 г. № 9)
составлена на основании учебного плана:

Направление: 01.03.02 Прикладная математика и информатика
утвержденного приказом ректора от 30.01.2024 № 32.

Рабочая программа одобрена на заседании кафедры

Информатики, математики и физики

Протокол от 21.03.2024 г. № 9

Срок действия программы: 2024 - 2028 уч.г.

Зав. кафедрой Горохов Д.Б.

Председатель МКФ Латушкина С.В.

Протокол от 26.04.2024 г. № 8

Ответственный за реализацию ОПОП _____ Горохов Д.Б.

Директор библиотеки _____ Сотник Т.Ф.

№ регистрации 45
(методический отдел)

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

_____ _____ 2025 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры
Информатики, математики и физики

Внесены изменения/дополнения (Приложение _____)

Протокол от _____ 2025 г. № __
Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

_____ __ _____ 2026 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры
Информатики, математики и физики

Внесены изменения/дополнения (Приложение _____)

Протокол от __ _____ 2026 г. № __
Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

_____ __ _____ 2027 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027-2028 учебном году на заседании кафедры
Информатики, математики и физики

Внесены изменения/дополнения (Приложение _____)

Протокол от __ _____ 2027 г. № __
Зав. кафедрой

Визирование РПД для исполнения в очередном учебном году

Председатель МКФ

_____ __ _____ 2028 г.

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2028-2029 учебном году на заседании кафедры
Информатики, математики и физики

Внесены изменения/дополнения (Приложение _____)

Протокол от __ _____ 2028 г. № __
Зав. кафедрой

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Получить устойчивые знания и навыки по обеспечению комплексной защиты объекта информатизации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В.04.ДВ.02.01
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Криптографические методы защиты информации
2.1.2	Основы информационной безопасности
2.1.3	Проектирование программного обеспечения
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Выполнение и защита выпускной квалификационной работы
2.2.2	Защита в операционных системах
2.2.3	Производственная (преддипломная) практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ПК-1: Способен проектировать компьютерное программное обеспечение	
Индикатор 1	ПК-1.1. Разрабатывает, изменяет архитектуру компьютерного программного обеспечения.
ПК-3: Способен администрировать системы защиты информации автоматизированных систем	
Индикатор 1	ПК-3.1. Выполняет работы по администрированию системы защиты информации автоматизированных систем.
Индикатор 1	ПК-3.2. Выполняет установленные процедуры обеспечения безопасности информации с учетом требования эффективного функционирования автоматизированной системы

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	программно-аппаратные средства защиты информации автоматизированных систем; методы контроля эффективности защиты информации от утечки по техническим каналам; критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем.
3.2	**Уметь:**
3.2.1	применять и администрировать программно-аппаратные средства защиты информации автоматизированных систем; регистрировать события, связанные с защитой информации в автоматизированных системах; анализировать события, связанные с защитой информации в автоматизированных системах.
3.3	**Владеть:**
3.3.1	навыками разработки организационно-функциональной структуры и комплекса нормативно-методического обеспечения безопасности объекта информатизации; технологиями обеспечения информационной безопасности; методы анализа и оценки угроз защищаемой информации в инфокоммуникационных системах.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Вид занятия	Наименование разделов и тем	Семестр / Курс	Часов	Компетен-ции	Литература	Инте ракт.	Примечание
	Раздел	**Раздел 1. Защита информации ограниченного доступа криптографическими средствами**						
1.1	Лек	Криптосистемы с открытым ключом, электронная подпись	7	2	ПК-3 ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-1.1, ПК-3.1, ПК-3.2
1.2	Лаб	Криптосистемы с открытым ключом, электронная подпись	7	2	ПК-3 ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-1.1, ПК-3.1, ПК-3.2

1.3	Лек	Хеш-функции. Обеспечение контроля целостности сообщений	7	2	ПК-3 ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	2	Лекция-дискуссия, ПК-1.1, ПК-3.1, ПК-3.2
1.4	Лаб	Хеш-функции. Обеспечение контроля целостности сообщений	7	2	ПК-3 ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-1.1, ПК-3.1, ПК-3.2
1.5	Лаб	Инфраструктура открытых ключей	7	2	ПК-3 ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-1.1, ПК-3.1, ПК-3.2
1.6	Лаб	Защита информации с использованием средств криптографической защиты	7	2	ПК-3 ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-1.1, ПК-3.1, ПК-3.2
1.7	Ср	Подготовка к выполнению ЛР	7	17	ПК-3 ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-1.1, ПК-3.1, ПК-3.2
1.8	Зачёт	Подготовка к зачёту	7	12	ПК-3 ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-1.1, ПК-3.1, ПК-3.2
	Раздел	**Раздел 2. Программные и программно-аппаратные средства защиты информации**						
2.1	Лек	Защищенная автоматизированная система	7	2	ПК-3 ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	2	Лекция-дискуссия, ПК-1.1, ПК-3.1, ПК-3.2
2.2	Лаб	Защищенная автоматизированная система	7	4	ПК-3 ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-1.1, ПК-3.1, ПК-3.2
2.3	Лек	Защита сетевого сегмента информационной системы корпоративного уровня	7	7	ПК-3 ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-1.1, ПК-3.1, ПК-3.2
2.4	Лаб	Защита сетевого сегмента информационной системы корпоративного уровня	7	10	ПК-3 ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	4	case-study (анализ конкретных ситуаций, ситуационный анализ), ПК-1.1, ПК-3.1, ПК-3.2

	Раздел	**Раздел 3. Техническая защита информации**						
3.1	Лек	Технические каналы утечки информации	7	2	ПК-3 ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-1.1, ПК-3.1, ПК-3.2
3.2	Лек	Методы добывания и защиты информации	7	2	ПК-3 ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	2	Лекция-дискуссия, ПК-1.1, ПК-3.1, ПК-3.2
3.3	Лаб	Технические средства и методы защиты информации	7	12	ПК-3 ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	2	case-study (анализ конкретных ситуаций, ситуационный анализ), ПК-1.1, ПК-3.1, ПК-3.2
3.4	Ср	Подготовка к выполнению ЛР	7	15	ПК-3 ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-1.1, ПК-3.1, ПК-3.2
3.5	Зачёт	Подготовка к зачёту	7	13	ПК-3 ПК-1	Л1.1 Л1.2 Л1.3 Л1.4Л2.1 Л2.2 Л2.3Л3.1 Л3.2	0	ПК-1.1, ПК-3.1, ПК-3.2

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Традиционная (репродуктивная) технология (преподаватель знакомит обучающихся с порядком выполнения задания, наблюдает за выполнением и при необходимости корректирует работу обучающихся)

Технология компьютерного обучения(использование в учебном процессе компьютерных технологий и предоставляемых ими возможностях (электронные библиотеки))

Образовательные технологии с использованием интерактивных методов обучения (case-study (анализ конкретных ситуаций))

Образовательные технологии с использованием интерактивных методов обучения (case-study (ситуационный анализ))

Образовательные технологии с использованием активных методов обучения (лекция – дискуссия)

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Контрольные вопросы и задания

ЛЕКЦИЯ-ДИСКУССИЯ
Лекция-дискуссия №1(2 час.)
Тема: Хеш-функции. Обеспечение контроля целостности сообщений.
Лекция-дискуссия №2(2 час.)
Тема: Защищенная автоматизированная система.
Лекция-дискуссия №3(2 час.)
Тема: Методы добывания и защиты информации.

CASE-STUDY (АНАЛИЗ КОНКРЕТНЫХ СИТУАЦИЙ, СИТУАЦИОННЫЙ АНАЛИЗ)
case-study (анализ конкретных ситуаций, ситуационны й анализ) №1.
Тема: Защита сетевого сегмента информационной системы корпоративного уровня.
case-study (анализ конкретных ситуаций, ситуационны й анализ) №2.
Тема: Технические средства и методы защиты информации.

ЛАБОРАТОРНЫЕ РАБОТЫ.
Лабораторная работа №1.
Тема: Криптосистемы с открытым ключом, электронная подпись.
Вопросы:
1)Основные виды электронной подписи;
2)Средства электронной подписи;
3)Сертификат ключа проверки электронной подписи;
4)Криптосистема RSA;
5)Криптосистема Эль-Гамаля.
Лабораторная работа №2.
Тема:Хеш-функции. Обеспечение контроля целостности сообщений.
Вопросы:
1)Хэш-функции SHA-1, SHA-2, SHA-3 и ГОСТ Р 34.11;
2)Контроль целостности сообщений;
Лабораторная работа №3.
Тема:Инфраструктура открытых ключей
Вопросы:
1)Основные понятия, термины и определения в области PKI;
2)Управление сертификатами и ключами;
3)Архитектура, основные компоненты PKI, их функции и взаимодействие;
4)Основные стандарты в области PKI: Стандарты серии X (X.509), стандарты криптографии с открытым ключом PKCS.
Лабораторная работа №4.
Тема:Защита информации с использованием средств криптографической защиты
Вопросы:
1)Защита автоматизированных систем предприятия с применением средств криптографической защиты;
2)Состав СКЗИ;
3)Структура СКЗИ;
4)Работа с ключевой информацией.
Лабораторная работа №5.
Тема:Защищенная автоматизированная система.
Вопросы:
1)Автоматизация процесса обработки информации. Понятие автоматизированной системы;
2)Особенности автоматизированных систем в защищенном исполнении;
4)Основные виды АС в защищенном исполнении;
5)Методы создания безопасных систем;
6)Методология проектирования гарантированно защищенных КС;
7)Дискреционные модели;
8)Мандатные модели.
Лабораторная работа №6.
Тема:Защита сетевого сегмента информационной системы корпоративного уровня.
Вопросы:
1) Работа с учётными записями пользователей и группами;
2) Настройка параметров мандатного управления доступом и мандатного контроля целостности;
3) Организация файловой системы ОССН для работы пользователей в рамках мандатного управления доступом и мандатного контроля целостности;
4) Администрирование ОССН в рамках реализации мандатного контроля целостности;
5) Настройка механизмов организации замкнутой программной среды;
6) Настройка сетевого взаимодействия;
Лабораторная работа №7.
Тема:Технические средства и методы защиты информации.
Вопросы:
1) Типовые структура и виды технических каналов утечки информации;
2) Основные показатели технических каналов утечки информации;
3) Комплексное использование технических каналов утечки информации;
4) Акустические и оптические каналы утечки информации;
5) Радиоэлектронные каналы утечки информации;
6) Вещественные каналы утечки информации;
7) Концепция инженерно-технической защиты информации;
8) Цели, задачи, ресурсы системы защиты информации;
9) Угрозы безопасности информации и меры по их предотвращению;
10) Принципы инженерно-технической защиты информации;
11) Принципы построения системы инженерно-технической защиты информации.

6.2. Темы письменных работ

Учебным планом не предусмотрено.

6.3. Фонд оценочных средств

Вопросы к зачёту:

Раздел 1. Защита информации ограниченного доступа криптографическими средствами.
1.1. Основные виды электронной подписи;
1.2. Средства электронной подписи;
1.3. Сертификат ключа проверки электронной подписи;
1.4. Криптосистема RSA;
1.5. Криптосистема Эль-Гамаля.
1.6. Хэш-функции SHA-1, SHA-2, SHA-3 и ГОСТ Р 34.11;
1.7. Контроль целостности сообщений;
1.8. Основные понятия, термины и определения в области PKI;
1.9. Управление сертификатами и ключами;
1.10. Архитектура, основные компоненты PKI, их функции и взаимодействие;
1.11. Основные стандарты в области PKI: Стандарты серии X (X.509), стандарты криптографии с открытым ключом PKCS;
1.12. Защита автоматизированных систем предприятия с применением средств криптографической защиты;
1.13. Состав и структура СКЗИ;
1.14. Работа с ключевой информацией.

Раздел 2. Программные и программно-аппаратные средства защиты информации.
2.1. Автоматизация процесса обработки информации. Понятие автоматизированной системы;
2.2. Особенности автоматизированных систем в защищенном исполнении;
2.3. Основные виды АС в защищенном исполнении;
2.4. Методы создания безопасных систем;
2.5. Методология проектирования гарантированно защищенных КС;
2.6. Дискреционные модели;
2.7. Мандатные модели.

Раздел 3. Техническая защита информации.
3.1. Типовые структура и виды технических каналов утечки информации;
3.2. Основные показатели технических каналов утечки информации;
3.3. Комплексное использование технических каналов утечки информации;
3.4. Акустические и оптические каналы утечки информации;
3.5. Радиоэлектронные каналы утечки информации;
3.6. Вещественные каналы утечки информации;
3.7. Концепция инженерно-технической защиты информации;
3.8. Цели, задачи, ресурсы системы защиты информации;
3.8. Угрозы безопасности информации и меры по их предотвращению;
3.9. Принципы инженерно-технической защиты информации;
3.10 Принципы построения системы инженерно-технической защиты информации.

6.4. Перечень видов оценочных средств

Отчеты по лабораторным работам; вопросы к зачёту.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л1.1	Ярочкин В.И.	Информационная безопасность: Учебник для вузов	Москва: Академический Проект, 2003	25	
Л1.2	Ищейнов В. Я.	Информационная безопасность и защита информации: теория и практика: учебное пособие	Москва|Берлин: Директ-Медиа, 2020	1	http://biblioclub.ru/index.php?page=book&id=571485
Л1.3	Ковалев Д. В., Богданова Е. А.	Информационная безопасность: учебное пособие	Ростов-на-Дону: Южный федеральный университет, 2016	1	http://biblioclub.ru/index.php?page=book&id=493175
Л1.4	Прохорова О. В.	Информационная безопасность и защита информации: учебник	Самара: Самарский государственный архитектурно-строительный университет, 2014	1	http://biblioclub.ru/index.php?page=book&id=438331

7.1.2. Дополнительная литература

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л2.1	Торокин А.А.	Инженерно-техническая защита информации: учебное пособие	Москва: Гелиос АРВ, 2005	10	
Л2.2	Титов А. А.	Технические средства защиты информации: учебное пособие	Томск: Томский государственный университет систем управления и радиоэлектроники, 2010	1	http://biblioclub.ru/index.php?page=book&id=208661
Л2.3	Титов А. А.	Инженерно-техническая защита информации: учебное пособие	Томск: Томский государственный университет систем управления и радиоэлектроники, 2010	1	http://biblioclub.ru/index.php?page=book&id=208567

7.1.3. Методические разработки

	Авторы,	Заглавие	Издательство,	Кол-во	Эл. адрес
Л3.1	Моргунов А. В.	Информационная безопасность: учебно-методическое пособие	Новосибирск: Новосибирский государственный технический университет, 2019	1	http://biblioclub.ru/index.php?page=book&id=576726
Л3.2	Кубашева Е. С., Малашкевич И. А., Чекулаева Е. Н.	Информатика и вычислительная техника. Информационная безопасность автоматизированных систем: учебно-методическое пособие	Йошкар-Ола: Поволжский государственный технологический университет, 2019	1	http://biblioclub.ru/index.php?page=book&id=562246

7.3.1 Перечень программного обеспечения

7.3.1.1	Microsoft Windows Professional 7 Russian Upgrade Academic OPEN No Level
7.3.1.2	Microsoft Office 2007 Russian Academic OPEN No Level
7.3.1.3	Adobe Acrobat Reader DC
7.3.1.4	Chrome
7.3.1.5	doPDF
7.3.1.6	LibreOffice

7.3.2 Перечень информационных справочных систем

7.3.2.1	Электронная библиотека БрГУ
7.3.2.2	Электронный каталог библиотеки БрГУ
7.3.2.3	«Университетская библиотека online»

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Аудитория	Назначение	Оснащение аудитории	Вид занятия
1346	Учебная аудитория (дисплейный класс)	Основное оборудование: - доска интерактивная Smart Board SB680; Системный блок Prime Box S302, 5-135000, 16GB DOR5,Gigabyte 4060, 1TBs5 D – 15 шт.; - Монитор Asus VA24E 23,8 - 15 шт.; - принтер HP LaserJet 1000 Series; - проектор Unifri35 (Vixuiti) SmartTechnologies; - коммутатор D-Link DES-1050G. Дополнительно: - маркерная доска - 1 шт. Учебная мебель: - комплект мебели (посадочных мест/АРМ) - 32/15 шт. - комплект мебели (посадочных мест) для преподавателя - 1 шт.	Лек
1346	Учебная аудитория (дисплейный класс)	Основное оборудование: - доска интерактивная Smart Board SB680; Системный блок Prime Box S302, 5-135000, 16GB DOR5,Gigabyte 4060, 1TBs5 D – 15 шт.; - Монитор Asus VA24E 23,8 - 15 шт.; - принтер HP LaserJet 1000 Series;	Лаб

		- проектор Unifri35 (Vixuiti) SmartTechnologies; - коммутатор D-Link DES-1050G. Дополнительно: - маркерная доска - 1 шт. Учебная мебель: - комплект мебели (посадочных мест/АРМ) - 32/15 шт. - комплект мебели (посадочных мест) для преподавателя - 1 шт.	
1346	Учебная аудитория (дисплейный класс)	Основное оборудование: - доска интерактивная Smart Board SB680; Системный блок Prime Box S302, 5-135000, 16GB DOR5,Gigabyte 4060, 1TBs5 D – 15 шт.; - Монитор Asus VA24E 23,8 - 15 шт.; - принтер HP LaserJet 1000 Series; - проектор Unifri35 (Vixuiti) SmartTechnologies; - коммутатор D-Link DES-1050G. Дополнительно: - маркерная доска - 1 шт. Учебная мебель: - комплект мебели (посадочных мест/АРМ) - 32/15 шт. - комплект мебели (посадочных мест) для преподавателя - 1 шт.	Зачёт
1101	Лаборатория теплоэнергетических систем	Основное оборудование: Стенд «Система солнечного нагрева с активной циркуляцией», Стенд «Система солнечного нагрева с пассивной циркуляцией», Стенд «Тепловой насос»; Дополнительно: Маркерная доска - 1 шт. Учебная мебель: Комплект мебели (посадочных мест) - 12 шт. Комплект мебели (посадочных мест) для преподавателя – 1 шт.	Ср

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина "Комплексное обеспечение безопасности объекта информатизации" направлена на совершенствование теоретических и практических навыков и умений в сфере обеспечения комплексной безопасности объектов информатизации критической и общегражданской инфраструктуры.

Лекции.

Написание конспекта лекций: краткое, последовательное изложение основных положений, формулировок, выводов, обобщений; техническое оформление записей (подчеркивание, выделение ключевых слов и терминов). Активная работа на лекции.

Лабораторные работы. Выполнение заданий с использованием методических рекомендаций по выполнению лабораторных работ, оформление отчетов, защита лабораторных работ.

Самостоятельная работа обучающихся. Подготовка к лабораторным работам: проработка материалов по теме лабораторной работы с использованием рекомендуемой литературы, конспекта лекций, ресурсов информационно-телекоммуникационной сети Интернет; выполнение заданий; оформление отчетов по лабораторным работам; подготовка к защите лабораторных работ.

Подготовка к зачёту: систематическая работа с конспектом лекций: чтение записей; проверка терминов с помощью энциклопедий, словарей и справочников; обозначение вопросов, материал, которых вызывает трудности; попытка найти ответ в рекомендуемых источниках; подготовка вопросов преподавателю, если не удается самостоятельно разобраться в материале.