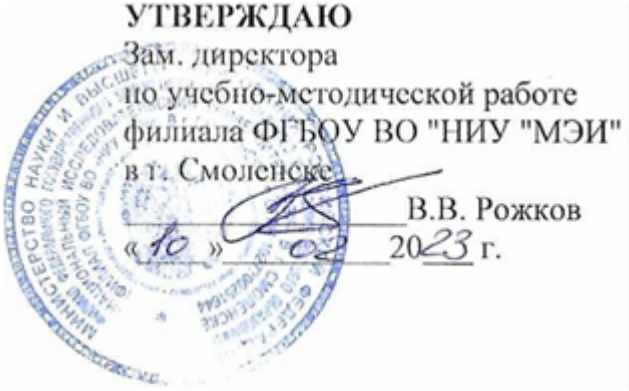
Филиал федерального государственного бюджетного образовательного учреждения высшего образования
«Национальный исследовательский университет «МЭИ»
в г. Смоленске



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

КОМПЛЕКСНАЯ ЗАЩИТА КОРПОРАТИВНОЙ ИНФОРМАЦИИ

(НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ)

Направление подготовки: 10.04.01 Информационная безопасность

Магистерская программа: Безопасность автоматизированных систем

Уровень высшего образования: магистратура

Нормативный срок обучения: 2 года

Форма обучения: очная

Год набора: 2023

Смоленск

Программа составлена с учетом ФГОС ВО – магистратура по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки России от «26» ноября 2020 г. № 1455.

Программу составил:

канд. экон. наук, доц. _____ О.В. Булыгина
подпись ФИО

«20» января 2023 г.

Программа обсуждена и одобрена на заседании кафедры информационных технологий в экономике и управлении
«07» февраля 2023 г., протокол № 6

Заведующий кафедрой информационных технологий в экономике и управлении:

_____ д-р техн. наук, проф. М.И. Дли
подпись ФИО

«08» февраля 2023 г.

Согласовано:

Заведующий кафедрой вычислительной техники:

_____ д-р техн. наук, проф. А.С. Федулов
подпись ФИО

«08» февраля 2023 г.

РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Ответственный в филиале по работе
с ЛОВЗ и инвалидами

_____ Е.В. Зуева
подпись ФИО

«08» февраля 2023 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является подготовка обучающихся к решению задач профессиональной деятельности организационно-управленческого типа в области защиты информации по направлению подготовки 10.04.01 Информационная безопасность (магистерская программа: Безопасность автоматизированных систем) посредством обеспечения этапов формирования компетенций, предусмотренных ФГОС и установленных программой магистратуры на основе профессиональных стандартов, в части представленных ниже знаний, умений и навыков.

Задачи дисциплины:

- ознакомить обучающихся с российскими нормативными правовыми актами, а также отечественными и зарубежными стандартами в области информационной безопасности и защиты информации;
- дать представление о современных инструментах обеспечения безопасности компьютерных систем и сетей;
- научить проводить анализ угроз безопасности компьютерных систем и сетей;
- сформировать навыки выявления проблем безопасности компьютерных систем и сетей;
- научить разрабатывать политики безопасности компьютерных систем и сетей;
- научить разрабатывать требования к системе комплексной защиты корпоративной информации;
- навыками разработки структуры системы комплексной защиты корпоративной информации;
- навыками подбора программно-аппаратных средств для построения системы комплексной защиты корпоративной информации;
- сформировать практические навыки расчета стоимости построения комплексной защиты корпоративной информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина Комплексная защита корпоративной информации относится *к части, формируемой участниками образовательных отношений.*

Для изучения данной дисциплины необходимы знания, умения и навыки, формируемые предшествующей дисциплиной:

Б1.В.01 Организационно-правовые механизмы обеспечения информационной безопасности
Б1.В.04 Информационная безопасность компьютерных сетей
Б1.В.07 Технические средства защиты информации

Знания, умения и навыки, формируемые данной дисциплиной необходимы для изучения следующих дисциплин, прохождения соответствующих видов практик и прохождения государственной итоговой аттестации:

Б1.В.ДВ.03.01 Безопасность веб-приложений
Б1.В.ДВ.03.02 Технологии и методы защиты информации в сети Интернет
Б2.В.02 (П) Проектно-технологическая практика
Б2.В.03 (П) Преддипломная практика
Б3.01 Подготовка к защите и защита выпускной квалификационной работы

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины направлено на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОП ВО по данному направлению подготовки:

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы достижения компетенций	Результаты обучения
ПК-3 Способен управлять безопасностью компьютерных систем и сетей	ПК-3.1 Проводит анализ безопасности компьютерных систем и сетей	Знает: принципы построения компьютерных систем и сетей. Умеет: проводить анализ угроз безопасности компьютерных систем и сетей. Владеет: навыками выявления проблем безопасности компьютерных систем и сетей.
	ПК-3.2 Разрабатывает требования по защите, формирует политики безопасности компьютерных систем и сетей	Знает: российские нормативные правовые акты, отечественные и зарубежные стандарты в области информационной безопасности и защиты информации. Умеет: разрабатывать требования к системе комплексной защиты корпоративной информации и формировать политики безопасности компьютерных систем и сетей. Владеет: навыками подбора программно-аппаратных средств для построения комплексной защиты корпоративной информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Структура дисциплины:

№	Индекс	Наименование	Семестр 3										Семестр 4										Итого за курс										Каф.	Семестры
			Контроль	Академических часов								з.е.	Недель	Контроль	Академических часов								з.е.	Недель	Контроль	Академических часов								з.е.	Недель		
				Всего	Конт такт.	Лек	Лаб	Пр	КРП	СР	Конт роль				Всего	Конт такт.	Лек	Лаб	Пр	КРП	СР	Конт роль				Всего	Конт такт.	Лек	Лаб	Пр	КРП	СР	Конт роль	Всего			
3	Б1.В.ДВ.02.01	Комплексная защита корпоративной информации	ЗаО РГР	**144**	86	34	34	18		40	18	4													ЗаО РГР	**144**	86	34	34	18		40	18	4		20	3

ОБОЗНАЧЕНИЯ:
Виды промежуточной аттестации (виды контроля):
Экз - экзамен;
ЗаО - зачет с оценкой;
За – зачет;
Виды работ:
Контакт. – контактная работа обучающихся с преподавателем;
Лек. – лекционные занятия;
Лаб.– лабораторные работы;
Пр. – практические занятия;
КРП – курсовая работа (курсовой проект);
РГР – расчетно-графическая работа (реферат);
СР – самостоятельная работа студентов;
з.е.– объем дисциплины в зачетных единицах.

Содержание дисциплины:

№	Наименование видов занятий и тематик, содержание
1	Лекционные занятия 17 шт. по 2 часа: 1.1. Принципы комплексной защиты корпоративной информации. 1.2. Стандартизация процессов защиты корпоративной информации. 1.3. Методология анализа защищенности информационной системы. 1.4. Политика безопасности корпоративных систем и сетей. 1.5. Обзор современных инструментов защиты корпоративной информации. 1.6. Физическая защита. 1.7. Защита цифровых АТС. 1.8. Защита операционных систем. 1.9. Защита от несанкционированного доступа. 1.10. Защита корпоративных информационных систем. 1.11. Защита web-приложений. 1.12. Защита корпоративных сетей организации. 1.13. Технологии виртуальных защищенных сетей. 1.14. Защита хранилищ корпоративных данных. 1.15. Защита систем электронного документооборота. 1.16. Криптографическая защита информации. 1.17. Организация защищенного межкорпоративного обмена.
2	Лабораторные работы 8 шт. по 4 часа и 1 шт. – 2 часа: 2.1. Проектирование структуры базы данных (2 часа). 2.2. Администрирование сервера баз данных (4 часа). 2.3. Создание базы данных в СУБД (4 часа). 2.4. Создание пользователей и выделение им привилегий (4 часа). 2.5. Организация ролевого управления доступом (4 часа). 2.6. Организация процедурного контроля целостности данных (4 часа). 2.7. Организация контроля ссылочной целостности данных (4 часа). 2.8. Управление доступом с помощью представлений (4 часа). 2.9. Резервное копирование и восстановление базы данных (4 часа).
3	Практические занятия 9 шт. по 2 часа: 3.1. Анализ безопасности компьютерных систем и сетей предприятия. 3.2. Построение модели угроз информационной безопасности. 3.3. Построение модели нарушителя. 3.4. Разработка функциональных требований к сервисам безопасности. 3.5. Разработка требований к адекватности реализации функций безопасности. 3.6. Разработка политики информационной безопасности предприятия. 3.7. Выбор программно-аппаратных средств построения системы комплексной защиты корпоративной информации. 3.8. Разработка структуры системы комплексной защиты корпоративной информации. 3.9. Расчет стоимости построения комплексной защиты корпоративной информации.
4	Расчетно-графическая работа «Разработка системы комплексной защиты корпоративной информации предприятия»
5	Самостоятельная работа студентов: 5.1. Безопасность персонала. 5.2. Электронная цифровая подпись.

	5.3. Межсетевое экранирование. 5.4. Защита корпоративной почтовой системы. 5.5. Безопасность электронной коммерции. 5.6. Выполнение расчетно-графической работы.

Текущий контроль:

Индикаторы достижения компетенции	**Вид текущего контроля**	**Тема**
ПК-3.1 Проводит анализ безопасности компьютерных систем и сетей	Проверка конспектов лекций Проверка выполнения заданий практических занятий Проверка отчета по расчетно-графической работе	1.3. Методология анализа защищенности информационной системы. 3.1. Анализ безопасности компьютерных систем и сетей предприятия. 3.2. Построение модели угроз информационной безопасности. 3.3. Построение модели нарушителя.
ПК-3.2 Разрабатывает требования по защите, формирует политики безопасности компьютерных систем и сетей	Проверка конспектов лекций и дополнительных материалов Защита лабораторных работ Проверка выполнения заданий практических занятий Проверка отчета по расчетно-графической работе	1.1. Принципы комплексной защиты корпоративной информации. 1.2. Стандартизация процессов защиты корпоративной информации. 1.4. Политика безопасности корпоративных систем и сетей. 1.5. Обзор современных инструментов защиты корпоративной информации. 1.6. Физическая защита. 1.7. Защита цифровых АТС. 1.8. Защита операционных систем. 1.9. Защита от несанкционированного доступа. 1.10. Защита корпоративных информационных систем. 1.11. Защита web-приложений. 1.12. Защита корпоративных сетей организации. 1.13. Технологии виртуальных защищенных сетей. 1.14. Защита хранилищ корпоративных данных. 1.15. Защита систем электронного документооборота. 1.16. Криптографическая защита информации. 1.17. Организация защищенного межкорпоративного обмена. 2.1. Проектирование структуры базы данных. 2.2. Администрирование сервера баз данных. 2.3. Создание базы данных в СУБД. 2.4. Создание пользователей и выделение им привилегий. 2.5. Организация ролевого управления доступом. 2.6. Организация процедурного контроля целостности данных. 2.7. Организация контроля ссылочной целостности данных.

		2.8. Управление доступом с помощью представлений. 2.9. Резервное копирование и восстановление базы данных. 3.4. Разработка функциональных требований к сервисам безопасности. 3.5. Разработка требований к адекватности реализации функций безопасности. 3.6. Разработка политики информационной безопасности предприятия. 3.7. Выбор программно-аппаратных средств построения системы комплексной защиты корпоративной информации. 3.8. Разработка структуры системы комплексной защиты корпоративной информации. 3.9. Расчет стоимости построения комплексной защиты корпоративной информации. 5.1. Безопасность персонала. 5.2. Электронная цифровая подпись. 5.3. Межсетевое экранирование. 5.4. Защита корпоративной почтовой системы. 5.5. Безопасность электронной коммерции.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Таблица - Образовательные технологии, используемые при реализации различных видов учебной занятий по дисциплине

№ п/п	Виды учебных занятий	Образовательные технологии
1	Лекции	Интерактивная лекция (лекция-визуализация) Индивидуальные и групповые консультации по дисциплине
2	Практические занятия	Проектная технология
3	Лабораторная работа	Технология выполнения лабораторных заданий индивидуально Проектная технология
4	Самостоятельная работа студентов (внеаудиторная)	Информационно-коммуникационные технологии (доступ к ЭИОС филиала, к ЭБС филиала, доступ к информационно-методическим материалам по дисциплине)
5	Контроль (промежуточная аттестация: зачет)	Технология устного опроса

6. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И

ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ – ДЛЯ ОЦЕНКИ КАЧЕСТВА ОСВОЕНИЯ ДИСЦИПЛИНЫ

К промежуточной аттестации студентов по дисциплине могут привлекаться представители работодателей, преподаватели последующих дисциплин, заведующие кафедрами.

Оценка качества освоения дисциплины включает как текущий контроль успеваемости, так и промежуточную аттестацию.

Вопросы для защиты лабораторной работы «Проектирование структуры базы данных»:

1. В чем концептуальная разница между логической и физической моделью данных?
2. Что включает в себя диаграмма сущность-связь?
3. Что включает в себя модель данных, основанная на ключах?
4. Какую информацию содержит трансформационная модель?
5. Что включает в себя полная атрибутная модель?

Вопросы для защиты лабораторной работы «Администрирование СУБД»:

1. Каковы особенности доступа в реляционных СУБД?
2. Привести примеры приложений для администрирования СУБД.
3. Какие типы кодировок используется в СУБД?
4. Для чего используются файлы состояний?
5. Как осуществляются запуск, остановка и перезагрузка сервера?

Вопросы для защиты лабораторной работы «Создание базы данных в СУБД»:

1. В чем заключается нормализация реляционной БД?
2. Какие типы ключей используются в реляционной модели БД?
3. Какие типы данных используются в СУБД?
4. Каким образом осуществляется создание индексов в СУБД?
5. Какова структура кода создания таблиц в СУБД?

Вопросы для защиты лабораторной работы «Создание пользователей и выделение им привилегий»:

1. Какие существуют основные категории пользователей СУБД?
2. Что такое набор ограничений доступа?
3. Какие виды привилегий применяются в СУБД?
4. Какие уровни привилегий существуют в СУБД?
5. Какими операторами происходит назначение и отмена привилегий в СУБД?

Вопросы для защиты лабораторной работы «Организация ролевого управления доступом»:

1. В чем состоит принцип ролевого управления доступом?
2. Каким образом влияет механизм ролей на повышение уровня информационной безопасности БД?
3. Как реализуется механизм ролей в СУБД?
4. Каков синтаксис SQL-операторов создания, изменения и удаления ролей в СУБД?
5. Каков синтаксис SQL-операторов предоставления привилегий доступа роли к объектам БД в СУБД?

Вопросы для защиты лабораторной работы «Организация процедурного контроля целостности данных»:

1. Какие существуют способы обеспечения целостности данных в БД?
2. В чем особенности декларативных способов обеспечения целостности данных в БД?
3. В чем особенности процедурных способов обеспечения целостности данных в БД?
4. В каких случаях триггер удаляется автоматически?
5. К каким событиям может быть привязан триггер?

Вопросы для защиты лабораторной работы «Организация контроля ссылочной целостности данных»:

1. Какие операции обработки данных способны нарушить ссылочную целостность?
2. Как механизм ссылочной целостность влияет на повышение уровня информационной безопасности БД?
3. Какие применяются стратегии для поддержания ссылочной целостности?
4. Как используется ограничение FOREIGN KEY при удалении/изменении информации в таблицах предках?
5. Как используется ограничение FOREIGN KEY при создании/изменении таблиц-потомков?

Вопросы для защиты лабораторной работы «Управление доступом с помощью представлений»:

1. Какую роль играет представление в контексте информационной безопасности?
2. Каков синтаксис оператора создания представления в СУБД?
3. В чем разница между вертикальными и горизонтальными представлениями?
4. Какие дополнительные конструкции содержит оператор создания представления в СУБД?
5. В каком виде хранятся в БД созданные представления?

Вопросы для защиты лабораторной работы «Резервное копирование и восстановление базы данных»:

1. Какие два подхода применяются для поддержания доступности БД?
2. В чем заключается постоянное дублирование данных и какие причины утраты информации оно устраняет?
3. Какие существуют методы безопасного создания резервных копий БД?
4. Что такое инкрементные бэкапы? Как они создаются, хранятся и используются?
5. В чем заключается механизм репликации БД в контексте задач резервного копирования? В чем заключаются его преимущества и недостатки?

Вопросы к защите проекта, выполняемого на практических занятиях:

1. Проводили ли Вы ранжирование угроз информационной безопасности?
2. Какие виды частных политик информационной безопасности Вы разрабатывали?
3. Какие подсистемы имеются в системе комплексной защиты корпоративной информации?
4. Какие инструменты Вы использовали для управления доступом?
5. Как Вы проводили расчет стоимости комплексной защиты корпоративной информации?

Результаты текущего контроля по вышеуказанным в разделе 4 видам фиксируются с использованием трехбалльной системы (0, 1, 2) в виде контрольных недель - при принятой в филиале системе на 6-й и 12-й учебной неделе семестра, а также учитываются преподавателем при

осуществлении промежуточной аттестации по настоящей дисциплине.

Форма промежуточной аттестации по настоящей дисциплине – *зачет с оценкой в 3-м семестре.*

Вопросы по закреплению теоретических знаний, умений и практических навыков, предусмотренных компетенциями (вопросы к зачету)

1. Проблемы безопасности корпоративной информации.
2. Принципы комплексной защиты корпоративной информации.
3. Стандартизация процессов защиты корпоративной информации.
4. Угрозы информационной безопасности в корпоративных системах и сетях.
5. Управление рисками информационной безопасности.
6. Методология анализа защищенности информационной системы.
7. Стратегия комплексного обеспечения информационной безопасности.
8. Политика безопасности корпоративных систем и сетей.
9. Требования к системе комплексной защиты корпоративной информации.
10. Структура системы комплексной защиты корпоративной информации.
11. Обзор современных инструментов защиты корпоративной информации.
12. Физическая защита.
13. Безопасность персонала.
14. Защита цифровых АТС.
15. Защита операционных систем.
16. Защита от несанкционированного доступа.
17. Защита корпоративных информационных систем.
18. Защита web-приложений.
19. Защита корпоративных сетей организации.
20. Межсетевое экранирование.
21. Технологии виртуальных защищенных сетей.
22. Защита хранилищ корпоративных данных.
23. Защита систем электронного документооборота.
24. Защита корпоративной почтовой системы.
25. Криптографическая защита информации.
26. Электронная цифровая подпись.
27. Организация защищенного межкорпоративного обмена.
28. Безопасность электронной коммерции.
29. Управление средствами обеспечения информационной безопасности.
30. Оценка стоимости комплексной защиты корпоративной информации.

Пример практических заданий, выносимых на зачет, для проверки практических умений и навыков студентов по дисциплине

Рассчитать общий уровень угроз по объекту защиты (сервер локальной сети) и итоговый риск. Критерий критичности равен 15 000 рублей.

Таблица - Угрозы и уязвимости

Угроза	Уязвимости
1.Физический доступ нарушителя к серверу	1.Неорганизованность контрольно-пропускного режима на предприятии

2.Отсутствие видеонаблюдения	1.Отсутствие соглашения о нераспространении
2.Разглашение информации, хранящейся на сервере	
2. Нечеткое распределение ответственности между сотрудниками предприятия	

Таблица - Уровни угрозы по определённой уязвимости и по всем уязвимостям

Угроза / уязвимость	Уровень угрозы по уязвимости	Уровень угрозы по всем уязвимостям
1/1	0,56	0,666
1/2	0,24	
2/1	0,09	0,408
2/2	0,35	

В филиале используется система с традиционной шкалой оценок – "отлично", "хорошо", "удовлетворительно", "неудовлетворительно", "зачтено", "не зачтено".

Применяемые критерии оценивания по дисциплинам (в соответствии с инструктивным письмом НИУ МЭИ от 14 мая 2012 года № И-23):

Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
«отлично»/ «зачтено (отлично)»/ «зачтено»	Выставляется обучающемуся, обнаружившему всестороннее, систематическое и глубокое знание материалов изученной дисциплины, умение свободно выполнять задания, предусмотренные программой, усвоивший основную и знакомый с дополнительной литературой, рекомендованной рабочей программой дисциплины; проявившему творческие способности в понимании, изложении и использовании материалов изученной дисциплины, безупречно ответившему не только на вопросы билета, но и на дополнительные вопросы в рамках рабочей программы дисциплины, правильно выполнившему практическое задание. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущего контроля. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «эталонный».
«хорошо»/ «зачтено (хорошо)»/ «зачтено»	Выставляется обучающемуся, обнаружившему полное знание материала изученной дисциплины, успешно выполняющему предусмотренные задания, усвоившему основную литературу, рекомендованную рабочей программой дисциплины; показавшему систематический характер знаний по дисциплине, ответившему на все вопросы билета, правильно выполнивший практическое задание, но допустивший при этом непринципиальные ошибки. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущего контроля. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «продвинутый».
«удовлетворительно»/ «зачтено (удовлетворительно)»/ «зачтено»	Выставляется обучающемуся, обнаружившему знание материала изученной дисциплины в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляющемуся с выполнением заданий, знакомому с основной литературой, рекомендованной рабочей программой дисциплины; допустившему погрешность в ответе на теоретические вопросы и/или при выполнении практических заданий, но обладающему необходимыми знаниями

Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
	для их устранения под руководством преподавателя, либо неправильно выполнившему практическое задание, но по указанию преподавателя выполнившему другие практические задания из того же раздела дисциплины.. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «пороговый».
«неудовлетворительно»/ не зачтено	Выставляется обучающемуся, обнаружившему серьезные пробелы в знаниях основного материала изученной дисциплины, допустившему принципиальные ошибки в выполнении заданий, не ответившему на все вопросы билета и дополнительные вопросы и неправильно выполнившему практическое задание (неправильное выполнение только практического задания не является однозначной причиной для выставления оценки «неудовлетворительно»). Как правило, оценка «неудовлетворительно ставится студентам, которые не могут продолжить обучение по образовательной программе без дополнительных занятий по соответствующей дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущего контроля. Компетенции на уровне «пороговый», закреплённые за дисциплиной, не сформированы.

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебное и учебно-лабораторное оборудование

Для проведения лекционных занятий

Учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная:

- специализированной мебелью; доской аудиторной; демонстрационным оборудованием: персональным компьютером (ноутбуком); переносным (стационарным) проектором.

Для проведения практических занятий

Учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная:

- специализированной мебелью; доской аудиторной; демонстрационным оборудованием: персональным компьютером (ноутбуком); переносным (стационарным) проектором.

Для проведения занятий лабораторного типа

Учебная аудитория для лабораторных работ, выполняемых в компьютерном классе, оснащенная:

- специализированной мебелью; доской аудиторной; персональными компьютерами с подключением к сети "Интернет".

Для самостоятельной работы обучающихся по дисциплине используется помещение для самостоятельной работы обучающихся, оснащенное:

- специализированной мебелью; доской аудиторной; персональным компьютерами с подключением к сети "Интернет" и доступом в ЭИОС филиала.

8. ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

В ходе реализации дисциплины используются следующие дополнительные методы 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;
- 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;
- используется специальная учебная аудитория для лиц с ЛОВЗ – ауд. 106 главного учебного корпуса по адресу 214013, г. Смоленск, Энергетический пр-д, д.1, здание энергетического института (основной корпус).

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 филиалом, 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.

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература.

1 Технологии обеспечения безопасности информационных систем [Электронный ресурс]: учебное пособие / А.Л. Марухленко, Л.О. Марухленко, М.А. Ефремов и др. – Москва; Берлин: Директ-Медиа, 2021. – 210 с. Режим доступа: https://biblioclub.ru/index.php?page=book&id=598988

2 Кияев В. Безопасность информационных систем [Электронный ресурс]: курс / В. Кияев, О. Граничин. – М.: Национальный Открытый Университет «ИНТУИТ», 2016. – 192 с. Режим доступа: https://biblioclub.ru/index.php?page=book&id=429032

Дополнительная литература.

1 Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций / А.В. Артемов. – Орел: Межрегиональная академия безопасности и выживания, 2014. – 257 с. Режим доступа: https://biblioclub.ru/index.php?page=book&id=428605

2 Голиков А.М. Защита информации в инфокоммуникационных системах и сетях [Электронный ресурс]: учебное пособие / А.М. Голиков. – Томск: Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с. Режим доступа: https://biblioclub.ru/index.php?page=book&id=480637

3 Прохорова О.В. Информационная безопасность и защита информации [Электронный ресурс]: учебник / О.В. Прохорова. – Самара: Самарский государственный архитектурно-строительный университет, 2014. – 113 с. Режим доступа: https://biblioclub.ru/index.php?page=book&id=438331

Список авторских методических разработок.

1 Булыгина О.В. Методические указания по выполнению практических занятий по дисциплине «Комплексная защита корпоративной информации».

2 Булыгина О.В. Методические указания по выполнению лабораторных работ по дисциплине «Комплексная защита корпоративной информации».

3 Булыгина О.В. Методические указания по выполнению расчетно-графической работы по дисциплине «Комплексная защита корпоративной информации».

Методические разработки по дисциплине расположены в ЭИОС филиала и на кафедральных ресурсах в ауд. 210

Перечень ресурсов информационно-телекоммуникационной сети «Интернет» необходимых для освоения дисциплины

1 Справочная правовая система Консультант плюс [электронный ресурс] — Режим доступа: http://www.consultant.ru/online/.

2 Официальный сайт Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) [электронный ресурс] — Режим доступа: http://government.ru/department/387/events/.

3 Официальный сайт Росстата [электронный ресурс] — Режим доступа: www.gks.ru/.

4 20 интернет-ресурсов для специалистов по информационной безопасности // официальный сайт компании «ГЕОЛАЙН Технологии» [электронный ресурс] — Режим доступа: http://geoline-tech.com/top-20-sites-about-information-security/.

5 Полезные сайты и инструменты// Информационная безопасность. Практика информационной безопасности [электронный ресурс] — Режим доступа: http://dorlov.blogspot.com/p/blog-page_3151.html.

6 Информационная безопасность [электронный ресурс] — Режим доступа: http://www.securrity.ru/.

7 30 ресурсов по безопасности, которые точно пригодятся [электронный ресурс] — Режим доступа: https://proglib.io/p/information-security-guide/

8 Информационная безопасность. Защита данных // habr - веб-сайт в формате коллективного блога с элементами новостного сайта [электронный ресурс] — Режим доступа: https://habr.com/ru/hub/infosecurity/.

9 База Знаний Клуба Информационной безопасности [электронный ресурс] — Режим доступа: http://wiki.informationsecurity.club/doku.php/main.

10 Информационная безопасность. Защита данных [электронный ресурс] — Режим доступа: http://all-ib.ru/

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ									
Номер изменения	Номера страниц				Всего страниц в документе	Наименование и № документа, вводящего изменения	Подпись, Ф.И.О. внесшего изменения в данный экземпляр	Дата внесения изменения в данный экземпляр	Дата введения изменения
	измененных	замененных	новых	аннулированных					
1	2	3	4	5	6	7	8	9	10