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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ТЕХНОЛОГИИ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

(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. _____ _____Д.Ю. Шутова_____
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: формирование умения обеспечить защиту информации и объектов информатизации; формирование навыков использования программно-аппаратных средств для защиты информации в сети Интернет.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина Технологии и методы защиты информации в сети Интернет 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
Б1.В.ДВ.02.01 Комплексная защита корпоративной информации
Б1.В.ДВ.02.02 Аудит информационной безопасности

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

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: угрозы информационной безопасности в сети Интернет; методы защиты компьютерных сетей от внешних угроз. Умеет: применять современные технологии обнаружения внешних вторжений; разрабатывать политику

		безопасности компьютерных сетей. Владеет: навыками использования программно-аппаратных средств для защиты информации в сети Интернет.
	ПК-3.2 Разрабатывает требования по защите, формирует политики безопасности компьютерных систем и сетей	Знать: основы управления информационной безопасностью компьютерных сетей; принципы безопасной работы в сети Интернет. Уметь: организовывать безопасную передачу данных в сети Интернет; разрабатывать требования к защите компьютерных систем и сетей Владеть: навыками администрирования программно-аппаратных средств защиты компьютерных сетей.

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			
6	*Б1.В.ДВ.03.02*	*Технологии и методы защиты информации в сети Интернет*	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. Угрозы информационной безопасности в сети Интернет (часть 1) 1.2. Угрозы информационной безопасности в сети Интернет (часть 2) 1.3. Принципы безопасного использования Интернет-ресурсов (часть 1) 1.4. Принципы безопасного использования Интернет-ресурсов (часть 2) 1.5. Технологии безопасной передачи информации в сети Интернет (часть 1) 1.6. Технологии безопасной передачи информации в сети Интернет (часть 2) 1.7. Защита от вредоносного программ и спама (часть 1) 1.8. Защита от вредоносного программ и спама (часть 2) 1.9. Межсетевое экранирование (часть 1) 1.10. Межсетевое экранирование (часть 2) 1.11. Организация виртуальных защищенных VPN-сетей (часть 1) 1.12. Организация виртуальных защищенных VPN-сетей (часть 2) 1.13. Понятие и классификация атак на компьютерные (часть 1) 1.14. Понятие и классификация атак на компьютерные (часть 2) 1.15. Методы обнаружения атак (часть 1) 1.16. Методы обнаружения атак (часть 2) 1.17. Системы обнаружения вторжений
2	Лабораторные работы 8 шт. по 4 часа и 1 шт. – 2 часа: 2.1. Защита от несанкционированного доступа и сетевых хакерских атак для ОС Windows 2.2. Управление доступом и защита ресурсов в системе Secret Net 2.3. Защита от несанкционированного доступа в системе Secret Net 2.4. Выявление признаков присутствия на компьютере вредоносных программ. Работа с командной строкой 2.5. Настройка сетевого экрана 2.6. Настройка виртуальных защищенных VPN-сетей 2.7. Регистрация и анализ сетевого трафика 2.8. Имитация сетевых атак 2.9. Работа с системой обнаружения вторжений
3	Практические занятия 9 шт. по 2 часа: 3.1. Информационная безопасность. Основные понятия. Модели информационной безопасности. Виды защищаемой информации. 3.2. Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны. 3.3. Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия. 3.4. Инженерная защита объектов. Защита информации от утечки по техническим каналам. 3.5. Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз. 3.6. Симметричные и ассиметричные системы шифрования. 3.7. Изучение настроек средств антивирусной защиты информации. 3.8. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы. 3.9. Политика безопасности. Экономическая безопасность предприятия.

4	Расчетно-графическая работа «Построение защиты компьютерной сети организации, подключенной к сети Интернет»
5	Самостоятельная работа студентов: 5.1 Криптографические методы защиты информации 5.2 Средства стеганографической защиты информации 5.3 Основные стандарты РФ в области информационной безопасности 5.4 Международные стандарты в области информационной безопасности 5.5 Правовое обеспечение информационной безопасности 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	Опрос Разбор конкретных ситуаций и групповые дискуссии по темам практических занятий Защита лабораторных работ Проверка выполнения заданий расчетно-графической работы Проверка отчета по расчетно-графической работе	1.1. Угрозы информационной безопасности в сети Интернет (часть 1) 1.2. Угрозы информационной безопасности в сети Интернет (часть 2) 1.3. Принципы безопасного использования Интернет-ресурсов (часть 1) 1.4. Принципы безопасного использования Интернет-ресурсов (часть 2) 1.5. Технологии безопасной передачи информации в сети Интернет (часть 1) 1.6. Технологии безопасной передачи информации в сети Интернет (часть 2)
ПК-3.2 Разрабатывает требования по защите, формирует политики безопасности компьютерных систем и сетей	Опрос Разбор конкретных ситуаций и групповые дискуссии по темам практических занятий Защита лабораторных работ Проверка выполнения заданий расчетно-графической работы Проверка отчета по расчетно-графической работе	1.8. Защита от вредоносного программ и спама (часть 2) 1.9. Межсетевое экранирование (часть 1) 1.10. Межсетевое экранирование (часть 2) 1.11. Организация виртуальных защищенных VPN-сетей (часть 1) 1.12. Организация виртуальных защищенных VPN-сетей (часть 2) 1.13. Понятие и классификация атак на компьютерные (часть 1) 1.14. Понятие и классификация атак на компьютерные (часть 2) 1.15. Методы обнаружения атак (часть 1) 1.16. Методы обнаружения атак (часть 2) 1.17. Системы обнаружения вторжений

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

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

№ п/п	Виды учебных занятий	Образовательные технологии
1	Лекции	Классическая (традиционная, информационная) лекция Интерактивная лекция (проблемная лекция) Индивидуальные и групповые консультации по дисциплине
2	Практические занятия	Технологии проведения практических занятий в форме семинара: тематический семинар Технология проблемного обучения на основе анализа ситуаций и имитационных моделей: групповая дискуссия, метод «круглого стола», работа малыми группами, командная работа, анализ-презентация Технология развития критического мышления: учебно-мозговой штурм, интеллектуальная разминка Технология обучения в сотрудничестве (командная, групповая работа)
3	Лабораторная работа	Технология выполнения лабораторных заданий индивидуально Проектная технология Допуск к лабораторной работе
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 Рейтинговая система контроля

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 «Защита от несанкционированного доступа и сетевых хакерских атак для ОС Windows»

1. Что такое брандмауэр?
2. Что такое статические и динамические IP-адреса?
3. Для чего используется диагностический запуск?

4. Что содержат файлы *SYSTEM.INI*, *WIN.INI* и *BOOT.INI*?

Вопросы для защиты лабораторной работы «Управление доступом и защита ресурсов в системе Secret Net».

1. Каково назначение системы *Secret Net*?
2. Какие механизмы управления доступом пользователей к ресурсам компьютера используются в системе *Secret N*et?
3. Каким образом можно временно заблокировать компьютер?
4. Какие режимы и соответствующие способы входа в систему существуют?

Вопросы для защиты лабораторной работы «Защита от несанкционированного доступа в системе Secret Net»

1. Какие пользователи имеют право изменять категорию конфиденциальности ресурсов в системе *Secret Net*?
2. Что представляет собой модель данных в системе *Secret Net*?
3. Каковы особенности функционирования механизма разграничения доступа к устройствам в «мягком» режиме?
4. Каковы особенности функционирования механизма разграничения доступа к устройствам в «жестком» режиме?

Вопросы для защиты лабораторной работы «Выявление признаков присутствия на компьютере вредоносных программ. Работа с командной строкой»

1. Назовите виды вредоносных программ.
2. Какая команда используется для получения информации о сетевой активности?
3. Для чего используются TCP-порты?
4. Для чего используются UDP-порты?

Вопросы для защиты лабораторной работы «Настройка сетевого экрана»

1. Для чего применяются межсетевые экраны?
2. Назовите две группы функций межсетевых экранов.
3. Объясните суть фильтрации потока межсетевым экраном.
4. От каких угроз не может защитить межсетевой экран?

Вопросы для защиты лабораторной работы «Настройка виртуальных защищенных VPN-сетей»

1. Поясните понятие «туннелирование».
2. Каковы функции инициатора и терминатора туннеля?
3. Какие методы используются для обеспечения безопасности VPN.
4. Что такое VPN-клиент, VPN-сервер и VPN-шлюз?

Вопросы для защиты лабораторной работы «Регистрация и анализ сетевого трафика»

1. Для чего используется команда Ping?
2. Перечислите преимущества и недостатки анализа потоков.
3. Перечислите преимущества и недостатки анализа «сырых» пакетов.
4. Какие задачи решают снифферы?

Вопросы для защиты лабораторной работы «Имитация сетевых атак»

1. Назовите виды сетевых атак.

2. Для чего используется RPC-сканирование?
3. Приведите примеры сетевых сканеров.
4. В чем заключается отличие DDoS от DoS атаки?

Вопросы для защиты лабораторной работы «Работа с системой обнаружения вторжений»

1. Для чего применяются системы обнаружения вторжений?
2. Поясните различие между атакой и аномалией?
3. Для чего используются сканеры уязвимостей?
4. Опишите суть сигнатурного анализа.

Вопросы для опроса и собеседования на практических занятиях

1. Что такое информационная безопасность?
2. Перечислите основные угрозы информационной безопасности.
3. Какие существуют модели информационной безопасности?
4. Какие методы защиты информации выделяют?
5. Основные уязвимости работы в сети Интернет.
6. Организационные меры защиты информации в сети Интернет.
7. Технологии безопасной передачи данных в сети Интернет.
8. Типы вредоносных программ.
9. Разновидности межсетевых экранов.
10. Уровни защищенных каналов.
11. Классификация атак на компьютерные сети.
12. Методы обнаружения злоупотреблений.
13. Методы обнаружения аномалий.
14. Классификация систем обнаружения вторжений.
15. Способы интеграции межсетевых экранов и систем обнаружения вторжений.

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. Угрозы информационной безопасности в сети Интернет.
2. Принципы безопасного использования Интернет-ресурсов.
3. Технологии безопасной передачи информации в сети Интернет.
4. Технические средства защиты информации в сети Интернет.
5. Организационные меры защиты информации в сети Интернет.
6. Отечественные и зарубежные стандарты информационной безопасности.
7. Основы управления информационной безопасностью компьютерных сетей

8. Защита от несанкционированного доступа.
9. Защита от вредоносных программ и спама.
10. Межсетевое экранирование.
11. Организация виртуальных защищенных VPN-сетей.
12. Классификация сетевых атак на компьютерные сети.
13. Методы обнаружения злоупотреблений и аномалий.
14. Системы обнаружения вторжений.

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

Задача 1

1. Какой должна быть маска подсети, чтобы IP-адрес 111.111.111.111 задавал 16 бит на подсеть и 16 бит на номер компьютера?
2. Каким должен быть IP-адрес и маска подсети, чтобы объединить 60000 компьютеров?
3. Сколько бит отводится на номер компьютера, если маска подсети 172.168.1.1?

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	Выставляется обучающемуся, обнаружившему знание материала изученной дисциплины в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляющемуся с выполнением заданий, знакомому с

Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
(удовлетворительно)»/ «зачтено»	основной литературой, рекомендованной рабочей программой дисциплины; допустившему погрешность в ответе на теоретические вопросы и/или при выполнении практических заданий, но обладающему необходимыми знаниями 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" и доступом в ЭИОС филиала

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 Камский В.А. Защита личной информации в Интернете, смартфоне и компьютере [Электронный ресурс]: учебное пособие / В.А. Камский. — Санкт-Петербург: Наука и Техника, 2017. — 272 с. — Режим доступа : https://e.lanbook.com/book/101559.

2 Марухленко А.Л. Технологии обеспечения безопасности информационных систем [Электронный ресурс]: учебное пособие / Л.А. 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

3 Технологии защиты информации в компьютерных сетях [Электронный ресурс] : учебное пособие / Н.А. Руденков [и др.]. — Москва: ИНТУИТ, 2016. — 368 с. — Режим доступа: https://e.lanbook.com/book/100522.

Дополнительная литература.

1 Сердюк В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий [Электронный ресурс] : учебное пособие. — Москва: Издательский дом Высшей школы экономики, 2015. — 574 с. — Режим доступа : http://biblioclub.ru/index.php?page=book&id=440285.

2 Лапонина О.Р. Протоколы безопасного сетевого взаимодействия [Электронный ресурс] . — 2-е изд., исправ. — Москва : Национальный Открытый Университет «ИНТУИТ», 2016. — 462 с. — Режим доступа : http://biblioclub.ru/index.php?page=book&id=429094.

3 Никифоров С.Н. Методы защиты информации. Защита от внешних вторжений [Электронный ресурс] : учеб. пособие / С.Н. Никифоров.— Санкт-Петербург : Лань, 2018. — 96 с. — Режим доступа: https://e.lanbook.com/book/107306.

4 Голиков А.М. Защита информации в инфокоммуникационных системах и сетях [Электронный ресурс]: учебное пособие / А.М. Голиков ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск: Томский государственный университет систем управления и радиоэлектроники, 2015. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=480637.

5 Булыгина О.В. Методические указания по выполнению расчетно-графической работы по дисциплине «Технологии и методы защиты информации в сети Интернет» [Электронный ресурс]: электронные методические указания для студентов, обучающихся по направлению 10.04.01 «Информационная безопасность» / Булыгина О.В. – Электрон. дан. – Смоленск: РИО филиала ФГБОУ ВО «НИУ «МЭИ» в г. Смоленске, 2019.

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