Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Национальный исследовательский университет «МЭИ»

Направление подготовки/специальность: 10.03.01 Информационная безопасность

Наименование образовательной программы: Безопасность компьютерных систем

Уровень образования: высшее образование - бакалавриат

Форма обучения: Очная

Рабочая программа дисциплины
ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ КИБЕРАТАК

Блок:	**Блок 1 «Дисциплины (модули)»**
Часть образовательной программы:	**Часть, формируемая участниками образовательных отношений**
№ дисциплины по учебному плану:	**Б1.Ч.10**
Трудоемкость в зачетных единицах:	**6 семестр - 6;**
Часов (всего) по учебному плану:	**216 часов**
Лекции	**6 семестр - 28 часа;**
Практические занятия	**6 семестр - 28 часа;**
Лабораторные работы	**6 семестр - 28 часа;**
Консультации	**6 семестр - 16 часов;**
Самостоятельная работа	**6 семестр - 111,2 часов;**
в том числе на КП/КР	**6 семестр - 10 часов;**
Иная контактная работа	**6 семестр - 4 часа;**
включая: **Контрольная работа**	
Промежуточная аттестация:	
Защита курсовой работы **Экзамен**	**6 семестр - 0,4 часа;** **6 семестр - 0,4 часа;** **всего - 0,8 часа**

Москва 2021

ПРОГРАММУ СОСТАВИЛ:

Преподаватель	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Дратвяк А.В. Идентификатор: R1a0ecc29-DratviakAV-b9b11303	А.В. Дратвяк
(должность)	(подпись)	(расшифровка подписи)

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)
Заведующий выпускающей кафедры	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. Идентификатор: R4bc65573-NevskyAY-0b6e493d	А.Ю. Невский
(должность, ученая степень, ученое звание)	(подпись)	(расшифровка подписи)

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины: освоение компетенций, связанных с изучением современного состояния и актуальности проблем кибербезопасности в России и мире. Изучение основных направлений деятельности по обеспечению безопасности системных и прикладных программных продуктов, а также web-приложений и ресурсов сети "Интернет" от киберугроз

Задачи дисциплины

- основание принципов администрирования программно-аппаратных средств защиты информации в компьютерных сетях для защиты от кибератак на информационные системы;
- обучение разработке требований к системе защиты автоматизированных систем и информационных ресурсов компании от кибератак;
- приобретение навыков по настройке и администрированию средств защиты от кибератак на информационные ресурсы хозяйствующего субъекта.

Формируемые у обучающегося **компетенции** и запланированные **результаты обучения** по дисциплине, соотнесенные с **индикаторами достижения компетенций**:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Запланированные результаты обучения**
ПК-3 Способен администрировать средства защиты информации в компьютерных системах и сетях	ПК-3.2$_{ПК-3}$ Администрирует программно-аппаратные средства защиты информации в компьютерных сетях	знать: - классификацию киберугроз информационной безопасности в соответствии нормативными документами регуляторов; - типовые алгоритмы атаки и механизмы защиты от кибератак на информационные системы; - программные и программно-аппаратные средства защиты компьютерных систем от кибератак. уметь: - проводить анализ угроз безопасности информационных систем в соответствии с международными и отечественными базами данных уязвимостей; - применять комплексные программные решения для тестирования, обнаружения и ликвидации киберугроз в информационных системах; - разрабатывать рекомендации по применению программных и программно-аппаратных решений для защиты системных и прикладных программных продуктов, а также web-приложений и ресурсов сети "Интернет" от киберугроз.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ ВО

Дисциплина относится к основной профессиональной образовательной программе Безопасность компьютерных систем (далее – ОПОП), направления подготовки 10.03.01 Информационная безопасность, уровень образования: высшее образование - бакалавриат.

Базируется на уровне среднего общего образования.

Результаты обучения, полученные при освоении дисциплины, необходимы при выполнении выпускной квалификационной работы.

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единиц, 216 часов.

№ п/п	Разделы/темы дисциплины/формы промежуточной аттестации	Всего часов на раздел	Семестр	Распределение трудоемкости раздела (в часах) по видам учебной работы										Содержание самостоятельной работы/ методические указания
				Контактная работа								СР		
				Лек	Лаб	Пр	Консультация		ИКР		ПА	Работа в семестре	Подготовка к аттестации /контроль	
							КПР	ГК	ИККП	ТК				
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Основы защиты информационных систем от кибератак	22	6	4	4	4	-	-	-	-	-	10	-	***Подготовка доклада, выступления:*** Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: ***Подготовка курсовой работы:*** Курсовая работа представлена в виде крупной задачи по учебному кейсу, охватывающей несколько расчетных вопросов и выбор варианта проектного решения. Пример задания: ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Основы защиты информационных систем от кибератак" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Основы защиты информационных систем от кибератак" ***Изучение материалов литературных источников:*** [3], 21-51
1.1	Введение в защиту от кибератак	11		2	2	2	-	-	-	-	-	5	-	
1.2	Модель угроз и модель нарушителя информационной безопасности в типовых информационных системах	11		2	2	2	-	-	-	-	-	5	-	

														[4], 5-89
2	Структура кибератаки на информационную систему объекта информатизации	65		12	12	12	-	-	-	-	-	29	-	***Подготовка доклада, выступления:*** Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных слайдов. В качестве тем докладов студентам предлагаются следующие варианты: ***Подготовка курсовой работы:*** Курсовая работа представлена в виде крупной задачи по учебному кейсу, охватывающей несколько расчетных вопросов и выбор варианта проектного решения. Пример задания: ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Структура кибератаки на информационную систему объекта информатизации" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Структура кибератаки на информационную систему объекта информатизации" ***Изучение материалов литературных источников:*** [1], 33-94 [2], 489-513 [4], 117-184
2.1	Атаки на корпоративные информационные системы компаний (КИС)	15		4	2	4	-	-	-	-	-	5	-	
2.2	Атаки на промышленные предприятия (АСУ ТП)	12		2	2	2	-	-	-	-	-	6	-	
2.3	Обнаружение атак на ИС	12		2	2	2	-	-	-	-	-	6	-	
2.4	Атаки на ИС. DoS/DDoS	12		2	2	2	-	-	-	-	-	6	-	
2.5	Атаки на ИС. Социальная инженерия	14		2	4	2	-	-	-	-	-	6	-	
3	Структура кибератаки на веб-приложения и ресурсы сети "Интернет"	64.7		12	12	12	-	-	-	-	-	28.7	-	***Подготовка доклада, выступления:*** Задание связано с углубленным изучением разделов дисциплины и самостоятельным поиском материалов для раскрытия темы доклада. Материалы выполненной работы представляются в электронном виде или в форме распечатанных презентационных
3.1	Выявление и эксплуатация SQL-инъекций в	15		4	2	4	-	-	-	-	-	5	-	

	приложениях													слайдов. В качестве тем докладов студентам предлагаются следующие варианты: ***Подготовка курсовой работы:*** Курсовая работа представлена в виде крупной задачи по учебному кейсу, охватывающей несколько расчетных вопросов и выбор варианта проектного решения. Пример задания: ***Подготовка к практическим занятиям:*** Изучение материала по разделу "Структура кибератаки на веб-приложения и ресурсы сети "Интернет"" подготовка к выполнению заданий на практических занятиях ***Самостоятельное изучение теоретического материала:*** Изучение дополнительного материала по разделу "Структура кибератаки на веб-приложения и ресурсы сети "Интернет" ***Изучение материалов литературных источников:*** [4], 241-375
3.2	Защита веб-приложений от инъекций команд	11		2	2	2	-	-	-	-	-	5	-	
3.3	Защита веб-приложений от атак типа XSS	12		2	2	2	-	-	-	-	-	6	-	
3.4	Меры предотвращения stored и reflected XSS. CSRF. SSRF.	12		2	2	2	-	-	-	-	-	6	-	
3.5	Применение подхода DevSecOps в современных системах разработки программного обеспечения	14.7		2	4	2	-	-	-	-	-	6.7	-	
	Экзамен	35.9		-	-	-	-	2	-	-	0.4	-	33.5	
	Курсовая работа (КР)	28.4		-	-	-	14	-	4	-	0.4	10	-	
	Всего за семестр	**216.0**		**28**	**28**	**28**	**14**	**2**	**4**	**-**	**0.8**	**77.7**	**33.5**	
	Итого за семестр	**216.0**		**28**	**28**	**28**	**16**		**4**		**0.8**	**111.2**		

Примечание: Лек – лекции; Лаб – лабораторные работы; Пр – практические занятия; КПР – аудиторные консультации по курсовым проектам/работам; ИККП – индивидуальные консультации по курсовым проектам/работам; ГК- групповые консультации по разделам дисциплины; СР – самостоятельная работа студента; ИКР – иная контактная работа; ТК – текущий контроль; ПА – промежуточная аттестация

3.2 Краткое содержание разделов

1. Основы защиты информационных систем от кибератак

1.1. Введение в защиту от кибератак

Понятие атаки на компьютерные системы. Классификация уязвимостей и кибератак. Примеры атак на компьютерные системы. База данных CVE и CWE. Ретроспектива киберинцидентов в России и мире. Описание реальных реализаций кибератак за предшествующий год. Вводная информация по темам предстоящих докладов: WannaCry, Stuxnet, NonPetya, Mirai, BEC, Zeus, Lazarus (атаки группировки), Industroyer, Cobalt, Dark Hotel, Turla (атаки группировки), DarkVishnya, KoffeyMaker и другая тема доклада на выбор студента (по согласованию с преподавателем).

1.2. Модель угроз и модель нарушителя информационной безопасности в типовых информационных системах

Модель угроз ФСТЭКа России. Цели злоумышленника. Квалификация злоумышленника. Основной инструментарий. Вводная информация по темам предстоящих докладов: создание модели нарушителя на конкретных примере типовой корпоративной инфраструктуры..

2. Структура кибератаки на информационную систему объекта информатизации

2.1. Атаки на корпоративные информационные системы компаний (КИС)

Типовая структура КИС с точки зрения безопасности. Примеры атак на КИС. Типовые защитные меры от кибератак на КИС. Вводная информация по темам предстоящих докладов: с учетом созданной модели нарушителя подобрать перечень защитных мер и обосновать его..

2.2. Атаки на промышленные предприятия (АСУ ТП)

Типовая структура АСУ ТП с точки зрения безопасности. Примеры атак на АСУ ТП. Типовые защитные меры. Вводная информация по темам предстоящих докладов: Разработка защитных мер для предприятия АСУ ТП на основе созданной модели нарушителя. Различия АСУ ТП и корпоративной ИС..

2.3. Обнаружение атак на ИС

Технология анализа атак на ИС. Методы обнаружения атак (признаки компрометации систем). Средства обнаружения атак (системы обнаружения вторжений). Вводная информация по темам предстоящих докладов: Подробный разбор технологии анализа атак (этапы, необходимая информация, средства и т.д.).

2.4. Атаки на ИС. DoS/DDoS

Понятие DoS/DDoS атаки, их особенность. Технология обнаружения атаки. Методы и средства защиты от DDoS. Вводная информация по темам предстоящих докладов: Детальный разбор методов и средств обнаружения и защиты от DoS/DDoS атак.

2.5. Атаки на ИС. Социальная инженерия

Понятие социальной инженерии, примеры. Технология обнаружения атаки. Методы и средства защиты от социальной инженерии. Вводная информация по темам предстоящих докладов: Подробное изучение методов социальной инженерии (фишинг, претекстинг и т.д.).

3. Структура кибератаки на веб-приложения и ресурсы сети "Интернет"

3.1. Выявление и эксплуатация SQL-инъекций в приложениях

Причины возникновения SQL-инъекций. Техники, применяемые при эксплуатации SQLинъекций. Процесс обнаружения и эксплуатации SQL-инъекций.

3.2. Защита веб-приложений от инъекций команд

Характеристика основ внедрения опасных команд. Методы обнаружения внедрения опасных команд. OWASP CheatSheet.

3.3. Защита веб-приложений от атак типа XSS

Общее понятие XSS. Виды XSS. Контексты выполнения. Common Weakness Enumeration.

3.4. Меры предотвращения stored и reflected XSS. CSRF. SSRF.

Меры предотвращения stored и reflected XSS. Меры предотвращения DOM-based XSS. Использование CSP..

3.5. Применение подхода DevSecOps в современных системах разработки программного обеспечения

Понятие DevSecOps. Организация фаззинга исходного кода. Сравнение некоторых SCA.

3.3. Темы практических занятий

1. 1 Введение в защиту от кибератак;
2. 2 Модель угроз и модель нарушителя информационной безопасности в типовых информационных системах;
3. 3 Атаки на корпоративные информационные системы компаний (КИС);
4. 4 Атаки на промышленные предприятия (АСУ ТП);
5. 5 Обнаружение атак на ИС;
6. 6 Атаки на ИС. DoS/DDoS;
7. 7 Атаки на ИС. Социальная инженерия;
8. 8 Выявление и эксплуатация SQL-инъекций в приложениях;
9. 9 Защита веб-приложений от инъекций команд;
10. 10 Защита веб-приложений от атак типа XSS;
11. 11 Меры предотвращения stored и reflected XSS. CSRF. SSRF.;
12. 12 Применение подхода DevSecOps в современных системах разработки программного обеспечения.

3.4. Темы лабораторных работ

1. 1. Исследование сервисов уязвимой виртуальной машины с применением CVE;
2. 2. Ознакомление с основным инструментарием злоумышленника на примере Kali Linux;
3. 3. Изучение возможностей применения инструмента Responder в ОС Kali Linux для выполнения атаки человек-посередине в отношении методов аутентификации в Windows;
4. 4. Установка и настройка IDS/IPS-системы Suricata и ELK;
5. 5. Администрирование IDS/IPS-системы Snort в целях противодействия кибератакам на автоматизированную систему;
6. 6. Знакомство с инструментами социальной инженерии на примере SET;
7. 7. Предотвращение атак, связанных с SQL-инъекциями;
8. 8. Предотвращение атак, связанных с инъекциями команд;

9. 9. Предотвращение атак, связанных с XSS. Часть 1;
10. 10. Предотвращение атак, связанных с XSS. Часть 1;
11. 11. Предотвращение атак, связанных с CSRF;
12. 12. Предотвращение Path/Directory Traversal и Open Redirect;
13. 13. Предотвращение встраивания веб-приложения в iframe на сайтах злоумышленника.

3.5 Консультации

Индивидуальные консультации по курсовому проету /работе (ИККП)

1. Консультации проводятся по разделу "Основы защиты информационных систем от кибератак"
2. Консультации проводятся по разделу "Структура кибератаки на информационную систему объекта информатизации"
3. Консультации проводятся по разделу "Структура кибератаки на веб-приложения и ресурсы сети "Интернет""

Текущий контроль (ТК)

1. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Основы защиты информационных систем от кибератак"
2. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Структура кибератаки на информационную систему объекта информатизации"
3. Консультации направлены на получение индивидуального задания для выполнения контрольных мероприятий по разделу "Структура кибератаки на веб-приложения и ресурсы сети "Интернет""

3.6 Тематика курсовых проектов/курсовых работ

6 Семестр

Курсовая работа (КР)
Темы:
- 1Особенности реализации защитных мер от кибератак для АСУ ТП на объектах КИИ 2Анализ методов обнаружения и предотвращения межсайтовой подделки запроса (CSRF) и подделки запроса на стороне сервера (SSRF) 3Анализ особенностей использования WAF для обнаружения и блокирования сетевых атак на веб-приложения 4Анализ последовательности работ по обнаружению и предотвращению кибератак с использованием механизма "выполнение" (execution) 5Анализ последовательности работ по обнаружению и предотвращению кибератак с использованием механизма "воздействие" (impact) 6Анализ последовательности работ по обнаружению и предотвращению кибератак с использованием механизма "начального доступа" (initial access) 7Анализ последовательности работ по обнаружению и предотвращению кибератак с использованием механизма "обход защиты" (defense evasion) 8Анализ последовательности работ по обнаружению и предотвращению кибератак с использованием механизма "перемещения внутри периметра" (lateral movement) 9Анализ последовательности работ по обнаружению и предотвращению кибератак с использованием механизма "повышение привилегий" (privilege escalation) 10Анализ последовательности работ по обнаружению и предотвращению кибератак с использованием механизма "получения учетных данных" (credential access) 11Анализ последовательности работ по обнаружению и предотвращению кибератак с использованием механизма "разведки" (discovery) 12Анализ последовательности работ по обнаружению и предотвращению кибератак с использованием механизма "сбора данных" (collection)

13Анализ последовательности работ по обнаружению и предотвращению кибератак с использованием механизма "управление и контроль" (command and control) 14Анализ последовательности работ по обнаружению и предотвращению кибератак с использованием механизма "эксфильтрация данных" (exfiltration) 15Анализ последовательности работ по обнаружению и предотвращению кибератак с использованием механизма "закрепление" (persistence) 16Анализ последовательности работ по предотвращению кибератак с использованием механизма "фиксации сессии" (session fixation) 17Анализ преимуществ использования межсетевых экранов нового поколения (NGFW, next-generation firewall) по сравнению с межсетевыми экранами предыдущих поколений 18Анализ соотношения требований по защищенности программного обеспечения от кибератак к уровню доверия 19Использование сканеров уязвимостей для защиты от кибератак 20Использование технологии SD-WAN security для предотвращения кибератак на примере виртуального маршрутизатора Cisco CSR1000v 21Методы обнаружения и предотвращения межсайтовой подделки запроса (CSRF) и подделки запроса на стороне сервера (SSRF) 22Организация процесса создания безопасной среды удаленной работы сотрудников 23Последовательность создания рабочих процессов в рамках методологии DevSecOps 24Применение метода очистки и экранирования пользовательских данных при реализации защитных мер от кибератак 25Применение метода противодействия APT (Advanced Persistent Threats) при организации защиты от кибератак на информационную систему предприятия 26Применение метода фильтрации и экранирования пользовательских данных при реализации защитных мер от кибератак типа внедрения 27Разработка алгоритма защиты информационной системы предприятия от кибератак с использованием средств обнаружения и предотвращения вторжений (IDS/IPS) 28Разработка и внедрение программ повышения осведомленности персонала (SAP), направленных на противодействие методам социальной инженерии 29Разработка и внедрение программного продукта, предназначенного для повышения осведомленности персонала от угроз социальной инженерии 30Разработка плана реагирования на кибератаки 31Разработка рекомендаций для защиты информационных систем от атак с применением методов социальной инженерии 32Разработка рекомендаций по настройке системы обнаружения вторжений для защиты сетей АСУ ТП 33Разработка рекомендаций по порядку внедрения и настройки средств обнаружения и предотвращения вторжений для защиты от кибератак 34Разработка рекомендаций по устранению уязвимости формы авторизации в веб-приложении 35Современные технологии и методы аутентификации в веб-приложениях 36Сравнительный анализ сканеров уязвимостей для защиты от кибератак 37Сравнительный анализ средств обнаружения и предотвращения вторжений для защиты от кибератак 38Формирование рекомендаций по обеспечению защиты от таргетированной атаки на информационную систему коммерческого предприятия. 39Формирование требований к комплексной системе защиты информации от кибератак с использованием систем обнаружения и предотвращения вторжений 40Формирование требований по использованию сканеров уязвимостей для защиты web-приложений от кибератак

График выполнения курсового проекта

Неделя	1 - 4	5 - 8	9 - 12	13 - 15	Зачетная
Раздел курсового проекта	1, 2	3, 4	4, 5	6, 7	Защита курсового проекта
Объем раздела, %	25	25	25	25	-
Выполненный объем нарастающим итогом, %	25	50	75	100	-

Номер раздела	Раздел курсового проекта
1	Титульный лист
2	Содержание
3	Введение
4	Первый раздел
5	Второй раздел
6	Заключение
7	Список использованной литературы

3.7. Соответствие разделов дисциплины и формируемых в них компетенций

Запланированные результаты обучения по дисциплине (в соответствии с разделом 1)	Коды индикаторов	Номер раздела дисциплины (в соответствии с п.3.1)			Оценочное средство (тип и наименование)
		1	2	3	
Знать:					
программные и программно-аппаратные средства защиты компьютерных систем от кибератак	ПК-3.2$_{ПК-3}$		+		Контрольная работа/Контрольное мероприятие № 2 Контрольная работа/Контрольное мероприятие № 3 Контрольная работа/Контрольное мероприятие № 6 Контрольная работа/Контрольное мероприятие № 7
типовые алгоритмы атаки и механизмы защиты от кибератак на информационные системы	ПК-3.2$_{ПК-3}$		+		Контрольная работа/Контрольное мероприятие № 4 Контрольная работа/Контрольное мероприятие № 8
классификацию киберугроз информационной безопасности в соответствии нормативными документами регуляторов	ПК-3.2$_{ПК-3}$	+			Контрольная работа/Контрольное мероприятие № 1 Контрольная работа/Контрольное

					мероприятие № 5
Уметь:					
разрабатывать рекомендации по применению программных и программно-аппаратных решений для защиты системных и прикладных программных продуктов, а также web-приложений и ресурсов сети "Интернет" от киберугроз	ПК-3.2$_{ПК-3}$			+	Контрольная работа/Контрольное мероприятие № 4 Контрольная работа/Контрольное мероприятие № 8
применять комплексные программные решения для тестирования, обнаружения и ликвидации киберугроз в информационных системах	ПК-3.2$_{ПК-3}$		+	+	Контрольная работа/Контрольное мероприятие № 1 Контрольная работа/Контрольное мероприятие № 5
проводить анализ угроз безопасности информационных систем в соответствии с международными и отечественными базами данных уязвимостей	ПК-3.2$_{ПК-3}$			+	Контрольная работа/Контрольное мероприятие № 2 Контрольная работа/Контрольное мероприятие № 3 Контрольная работа/Контрольное мероприятие № 6 Контрольная работа/Контрольное мероприятие № 7

4. КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ДИСЦИПЛИНЕ)

4.1. Текущий контроль успеваемости

6 семестр

Форма реализации: Письменная работа

1. Контрольное мероприятие № 1 (Контрольная работа)
2. Контрольное мероприятие № 2 (Контрольная работа)
3. Контрольное мероприятие № 3 (Контрольная работа)
4. Контрольное мероприятие № 4 (Контрольная работа)
5. Контрольное мероприятие № 5 (Контрольная работа)
6. Контрольное мероприятие № 6 (Контрольная работа)
7. Контрольное мероприятие № 7 (Контрольная работа)
8. Контрольное мероприятие № 8 (Контрольная работа)

Балльно-рейтинговая структура дисциплины является приложением А.
Балльно-рейтинговая структура курсовой работы является приложением Б.

4.2 Промежуточная аттестация по дисциплине

Экзамен (Семестр №6)

Курсовая работа (КР) (Семестр №6)

Результат работы в семестре оценивается с учётом выполнения сроков поэтапной сдачи разделов курсовой работы, посещения консультаций, а также правильности изложенных в курсовой работе теоретического и практического аспектов темы работы

Примечание: Оценочные материалы по дисциплине приведены в фонде оценочных материалов ОПОП.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1 Печатные и электронные издания:

1. Кибербезопасность цифровой индустрии : теория и практика функциональной устойчивости к кибератакам / Д. П. Зегжда, Е. Б. Александрова, М. О. Калинин, [и др.] ; ред. Д. П. Зегжда . – Москва : Горячая Линия-Телеком, 2020 . – 560 с. - Авторы указаны на обороте тит. л. - ISBN 978-5-9912-0827-7 .;
2. Белоус, А. И. Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения / А. И. Белоус . – Москва; Вологда : Инфра-Инженерия, 2020 . – 644 с. - ISBN 978-5-9729-0512-6 .;
3. Управление событиями информационной безопасности : учебное пособие / А. С. Минзов, О. Р. Баронов, С. А. Минзов, П. А. Осипов, Нац. исслед. ун-т "МЭИ" (НИУ"МЭИ"), Инженерно-экономич. ин-т национального исслед. ун-та "МЭИ" ; ред. А. Ю. Невский . – Москва : ВНИИгеосистем, 2020 . – 110 с. - Для студентов бакалавриата, магистратуры, аспирантов и преподавателей, занимающихся вопросами создания эффективных систем управления кибербезопасностью . - ISBN 978-5-8481-0244-4 .;
4. Диогенес Ю., Озкайя Э.- "Кибербезопасность. стратегия атак и обороны", Издательство: "ДМК Пресс", Москва, 2020 - (326 с.)
https://e.lanbook.com/book/131717.

5.2 Лицензионное и свободно распространяемое программное обеспечение:
1. СДО "Прометей";
2. Office;
3. Windows;
4. Майнд Видеоконференции;
5. Windows Server;
6. Kali Linux.

5.3 Интернет-ресурсы, включая профессиональные базы данных и информационно-справочные системы:
1. **ЭБС Лань** - https://e.lanbook.com/
2. **ЭБС "Университетская библиотека онлайн"** - http://biblioclub.ru/index.php?page=main_ub_red
3. **Научная электронная библиотека** - https://elibrary.ru/
4. **База данных Web of Science** - http://webofscience.com/
5. **База данных Scopus** - http://www.scopus.com
6. **ЭБС "Консультант студента"** - http://www.studentlibrary.ru/
7. **Журнал Science** - https://www.sciencemag.org/
8. **Электронная библиотека МЭИ (ЭБ МЭИ)** - http://elib.mpei.ru/login.php
9. **Информационно-справочная система «Кодекс/Техэксперт»** - Http:\\proinfosoft.ru; http://docs.cntd.ru/
10. **Национальный портал онлайн обучения «Открытое образование»** - https://openedu.ru
11. **Открытая университетская информационная система «РОССИЯ»** - https://uisrussia.msu.ru
12. **Федеральный портал "Российское образование"** - http://www.edu.ru

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Тип помещения	Номер аудитории, наименование	Оснащение
Учебные аудитории для проведения лекционных занятий и текущего контроля	Н-204, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, колонки звуковые, мультимедийный проектор, экран
	К-601, Учебная аудитория	парта со скамьей, стол преподавателя, стул, трибуна, доска меловая, мультимедийный проектор, экран
Учебные аудитории для проведения практических занятий, КР и КП	М-511, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
Учебные аудитории для проведения промежуточной аттестации	М-511, Учебная аудитория	парта, стол преподавателя, стул, доска меловая
	Ж-120, Машинный зал ИВЦ	сервер, кондиционер
Помещения для самостоятельной работы	НТБ-303, Компьютерный читальный зал	стол компьютерный, стул, стол письменный, вешалка для одежды, компьютерная сеть с выходом в Интернет, компьютер персональный, принтер, кондиционер
Помещения для консультирования	А-300, Учебная аудитория "А"	кресло рабочее, парта, стеллаж, стол преподавателя, стол учебный, стул, трибуна, микрофон, мультимедийный проектор,

		экран, доска маркерная, колонки, техническая аппаратура, кондиционер, телевизор
Помещения для хранения оборудования и учебного инвентаря	К-202/2, Склад кафедры БИТ	стеллаж для хранения инвентаря, стол, стул, шкаф для документов, шкаф для хранения инвентаря, тумба, запасные комплектующие для оборудования

Приложение А

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА ДИСЦИПЛИНЫ

Технологии защиты информационных систем от кибератак

(название дисциплины)

6 семестр

Перечень контрольных мероприятий <u>текущего контроля</u> успеваемости по дисциплине:

КМ-1 Контрольное мероприятие № 1 (Контрольная работа)
КМ-2 Контрольное мероприятие № 2 (Контрольная работа)
КМ-3 Контрольное мероприятие № 3 (Контрольная работа)
КМ-4 Контрольное мероприятие № 4 (Контрольная работа)
КМ-5 Контрольное мероприятие № 5 (Контрольная работа)
КМ-6 Контрольное мероприятие № 6 (Контрольная работа)
КМ-7 Контрольное мероприятие № 7 (Контрольная работа)
КМ-8 Контрольное мероприятие № 8 (Контрольная работа)

Вид промежуточной аттестации – Экзамен.

Номер раздела	Раздел дисциплины	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4	КМ-5	КМ-6	КМ-7	КМ-8
		Неделя КМ:	2	4	6	8	10	12	14	15
1	Основы защиты информационных систем от кибератак									
1.1	Введение в защиту от кибератак		+				+			
1.2	Модель угроз и модель нарушителя информационной безопасности в типовых информационных системах		+				+			
2	Структура кибератаки на информационную систему объекта информатизации									
2.1	Атаки на корпоративные информационные системы компаний (КИС)			+	+			+	+	
2.2	Атаки на промышленные предприятия (АСУ ТП)			+	+			+	+	
2.3	Обнаружение атак на ИС					+				+
2.4	Атаки на ИС. DoS/DDoS					+				+
2.5	Атаки на ИС. Социальная инженерия		+				+			
3	Структура кибератаки на веб-приложения и ресурсы сети "Интернет"									

3.1	Выявление и эксплуатация SQL-инъекций в приложениях	+				+			
3.2	Защита веб-приложений от инъекций команд		+	+			+	+	
3.3	Защита веб-приложений от атак типа XSS		+	+			+	+	
3.4	Меры предотвращения stored и reflected XSS. CSRF. SSRF.				+				+
3.5	Применение подхода DevSecOps в современных системах разработки программного обеспечения				+				+
	Вес КМ, %:	12,5	12,5	12,5	12,5	12,5	12,5	12,5	12,5

Приложение Б

БАЛЛЬНО-РЕЙТИНГОВАЯ СТРУКТУРА КУРСОВОГО ПРОЕКТА/РАБОТЫ ПО ДИСЦИПЛИНЕ

Технологии защиты информационных систем от кибератак

(название дисциплины)

6 семестр

Перечень контрольных мероприятий <u>текущего контроля</u> успеваемости по курсовой работе:

КМ-1 Утверждение темы и содержания
КМ-2 Оформление введения и первого раздела
КМ-3 Оформление первого и второго разделов
КМ-4 Оформление заключения и списка литературы

Вид промежуточной аттестации – защита КР.

Номер раздела	Раздел курсового проекта/курсовой работы	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
		Неделя КМ:	4	8	12	15
1	Титульный лист		+			
2	Содержание		+			
3	Введение			+		
4	Первый раздел			+	+	
5	Второй раздел				+	
6	Заключение					+
7	Список использованной литературы					+
		Вес КМ, %:	25	25	25	25