Министерство науки и высшего образования Российской Федерации

Муромский институт (филиал)

федерального государственного бюджетного образовательного учреждения высшего образования

«Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»

(МИ ВлГУ)

Кафедра *УКТС*

«УТВЕРЖДАЮ»
Заместитель директора по УР
_____Д.Е. Андрианов
21.05.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность и защита информации

Направление подготовки *11.03.02 Инфокоммуникационные технологии и системы связи*

Профиль подготовки *Интеллектуальная электроника и высокоуровневый интернет вещей*

Семестр	Трудоемкость, час./зач. ед.	Лекции, час.	Практические занятия, час.	Лабораторные работы, час.	Консультация, час.	Контроль, час.	Всего (контактная работа), час.	СРС, час.	Форма промежуточного контроля (экз., зач., зач. с оц.)
6	**144 / 4**	**16**	**16**	**16**	**3,6**	**0,35**	**51,95**	**65,4**	**Экз.(26,65)**
Итого	**144 / 4**	**16**	**16**	**16**	**3,6**	**0,35**	**51,95**	**65,4**	**26,65**

Муром, 2024 г.

1. Цель освоения дисциплины

Цель дисциплины: подготовить специалистов, способных внедрять и применять решения на базе ИИ для защиты корпоративной инфраструктуры, предотвращения кибератак и соблюдения этических норм при работе с данными.

Задачи:

- обучение применению технологий информационной безопасности;
- изучение методов защиты данных и предотвращения утечек;
- освещение вопросов этики при разработке и внедрении ИИ в информационные системы;
- изучение угроз, связанных с применением ИИ в кибератаках, и разработка методов противодействия;
- подготовка к использованию анализа данных для обнаружения угроз и автоматизации управления безопасностью.

2. Место дисциплины в структуре ОПОП ВО

Курс базируется на дисциплинах: устройства и системы беспроводной передачи данных; интернет вещей; системы беспроводной связи; основы программирования и баз данных и других. Базирующимися дисциплинами являются: хранилища данных и облачные технологии; искусственный интеллект; интеллектуальная обработка мультимедиа трафика и другие.

3. Планируемые результаты обучения по дисциплине

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции	Результаты обучения по дисциплине	
ПК-3 Спопособен анализировать внутресетевое взаимодействие и применять методы искусственного интеллекта для обработки и анализа передаваемых данных и сетевого трафика	ПК-3.2 Анализирует внутресетевые взаимодействия	Методы и технологии анализа киберугроз и аномалий, в том числе с использованием ИИ (ПК-3.2) Анализировать риски информационной безопасности и уязвимости корпоративных систем с применением аналитических инструментов (ПК-3.2) Навыками анализа киберугроз и их предотвращения (ПК-3.2)	отчет, тест
ОПК-3 Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности	ОПК-3.3 Соблюдает требования информационной безопасности	Основные нормативные правовые акты в области применения ИИ и защиты данных (ОПК-3.3) Выбирать решения по защите данных с учетом требований информационной безопасности (ОПК-3.3) Навыками разработки и внедрения решений для защиты сетей и систем (ОПК-3.3)	отчет, тест

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы, 144 часа.

4.1. Форма обучения: очная

Уровень базового образования: среднее общее.
Срок обучения 4г.

4.1.1. Структура дисциплины

№ п\п	Раздел (тема) дисциплины	Семестр	Контактная работа обучающихся с педагогическим работником							Самостоятельная работа	Форма текущего контроля успеваемости (по неделям семестра), форма промежуточной аттестации(по семестрам)
			Лекции	Практические занятия	Лабораторные работы	Контрольные работы	КП / КР	Консультация	Контроль		
1	Угрозы информационный безопасности	6	8	2	4					12	отчет, тестирование
2	Защита информации	6	8	14	12					53,4	отчет, тестирование
Всего за семестр		144	16	16	16			3,6	0,35	65,4	Экз.(26,65)
Итого		144	16	16	16			3,6	0,35	65,4	26,65

4.1.2. Содержание дисциплины

4.1.2.1. Перечень лекций

Семестр 6

Раздел 1. Угрозы информационный безопасности

Лекция 1.

Основные понятия, государственные структуры и стандарты (2 часа).

Лекция 2.

Природа возникновения угроз и классификация угроз (2 часа).

Лекция 3.

Угрозы безопасности информационной системы (2 часа).

Лекция 4.

Уязвимость программных приложений (2 часа).

Раздел 2. Защита информации

Лекция 5.

Методы противодействия несанкционированному доступу (2 часа).

Лекция 6.

Политика безопасности (2 часа).

Лекция 7.

Криптографическая защита (2 часа).

Лекция 8.

Защита информации в глобальных сетях (2 часа).

4.1.2.2. Перечень практических занятий

Семестр 6

Раздел 1. Угрозы информационный безопасности

Практическое занятие 1

Анализ сетевой безопасности (2 часа).

Раздел 2. Защита информации

Практическое занятие 2

Конфигурация брандмауэра (2 часа).

Практическое занятие 3

Анализ журналов безопасности (2 часа).

Практическое занятие 4

Настройка политики безопасности (2 часа).

Практическое занятие 5

Настройка протокола безопасности IPSec (2 часа).

Практическое занятие 6

Изучение методов шифрования (2 часа).

Практическое занятие 7

Симметричные криптосистемы (2 часа).

Практическое занятие 8

Несимметричные криптосистемы (2 часа).

4.1.2.3. Перечень лабораторных работ

Семестр 6

Раздел 1. Угрозы информационный безопасности

Лабораторная 1.

Симуляция атаки и защита (4 часа).

Раздел 2. Защита информации

Лабораторная 2.

Защита от DDoS-атак (4 часа).

Лабораторная 3.

Программная реализация методов шифрования (4 часа).

Лабораторная 4.

Разработка плана реагирования на инциденты безопасности (4 часа).

4.1.2.4. Перечень тем и учебно-методическое обеспечение самостоятельной работы

Перечень тем, вынесенных на самостоятельное изучение:

1. Взлом и анализ уязвимостей веб-приложения: проведение атак и устранение уязвимостей веб-приложений с использованием инструментов типа OWASP ZAP или Burp Suite.
2. Анализ защищенности сети: проверка сетевой инфраструктуры на уязвимости и разработка рекомендаций по устранению обнаруженных уязвимостей.
3. Криптоанализ: изучение методов взлома шифрования и проведение практических исследований в области криптоанализа.
4. Программирование безопасных приложений: создание и аудит безопасных приложений, включая защиту от инъекций, утечек данных, и других угроз.
5. Мониторинг безопасности: установка и настройка систем мониторинга безопасности для сетевых устройств и сбор логов для дальнейшего анализа.
6. Симуляция кибератак: проведение симуляции кибератак для оценки уровня защищенности сети и разработки планов реагирования на инциденты.

7. Защита мобильных устройств: анализ угроз для мобильных платформ, разработка и тестирование методов защиты от вредоносных приложений, перехвата данных и несанкционированного доступа.
8. Создание политики безопасности: разработка политики информационной безопасности для организации, включая аудит бизнес-процессов и разработку процедур реагирования на инциденты.
9. Защита от социальной инженерии: проведение тренинга по защите от социальной инженерии и анализ рисков, связанных с человеческим фактором в информационной безопасности.
10. Информационная безопасность для Интернета вещей: разработка и тестирование методов защиты и управления рисками в сфере интернета вещей.

Для самостоятельной работы используются методические указания по освоению дисциплины и издания из списка приведенной ниже основной и дополнительной литературы.

4.1.2.5. Перечень тем контрольных работ, рефератов, ТР, РГР, РПР

Не планируется.

4.1.2.6. Примерный перечень тем курсовых работ (проектов)

Не планируется.

5. Образовательные технологии

В процессе изучения дисциплины применяется контактная технология преподавания (за исключением самостоятельно изучаемых студентами вопросов). При проведении занятий применяется имитационный или симуляционный подход, когда преподавателем разбирается на конкретном примере проблемная ситуация, все шаги решения задачи студентам демонстрируются при помощи мультимедийной техники. Затем студенты самостоятельно решают аналогичные задания. Так же при проведении занятий применяется частично-поисковый метод: студенты осуществляют поиск решения поставленной проблемы (задачи). При этом, постановочные задачи опираются на уже имеющиеся у студентов знания и умения, полученные в предшествующих темах.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины.

Фонды оценочных материалов (средств) приведены в приложении.

7. Учебно-методическое и информационное обеспечение дисциплины.

7.1. Основная учебно-методическая литература по дисциплине

1. Авдошин С.М. Технологии и продукты Microsoft в обеспечении информационной безопасности [Электронный ресурс]: учебное пособие/ Авдошин С.М., Савельева А.А., Сердюк В.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021.— 431 c. - https://www.iprbookshop.ru/102070.html

2. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 154 c. - https://www.iprbookshop.ru/133957.html

3. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 266 c. - https://www.iprbookshop.ru/142285.html

7.2. Дополнительная учебно-методическая литература по дисциплине

1. Артемов А.В. Информационная безопасность : курс лекций / Артемов А.В.. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 256 c. - https://www.iprbookshop.ru/33430.html

2. Башлы, П. Н. Информационная безопасность и защита информации : учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — Москва : Евразийский открытый институт, 2012. — 311 c. - https://www.iprbookshop.ru/10677.html

7.3. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

В образовательном процессе используются информационные технологии, реализованные на основе информационно-образовательного портала института (www.mivlgu.ru/iop), и инфокоммуникационной сети института:

- предоставление учебно-методических материалов в электронном виде;
- взаимодействие участников образовательного процесса через локальную сеть института и Интернет;
- предоставление сведений о результатах учебной деятельности в электронном личном кабинете обучающегося.

Информационные справочные системы:

Форум специалистов по информационным технологиям http://citforum.ru/

Интернет-университет информационных технологий http://www.intuit.ru/

Тематический форум по информационным технологиям http://habrahabr.ru/

Программное обеспечение:

Microsoft Windows 7 Professional (Программа Microsoft Azure Dev Tools for Teaching (Order Number: IM126433))

Python 3.9.4 (Python Software Foundation License)

Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition (Договор №436 от 11.11.2014 года)

Open Office (Бесплатное ПО)

NetTraffic Version 2.0 (Бесплатное ПО)

Friendly Pinger 5.0.1 (Бесплатное ПО)

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

iprbookshop.ru

citforum.ru

intuit.ru

habrahabr.ru

mivlgu.ru/iop

8. Материально-техническое обеспечение дисциплины

Лаборатория компьютерного моделирования в измерительных системах

ЭВМ Айтек Intel Core i5 2400 - 12 шт.; Лабораторный стенд изучение интерфейсов сопряжения – 12 шт. ; Видеопроектор Acer P1100 EY; Экран настенный ScreenMedia Economy-P.

9. Методические указания по освоению дисциплины

Для успешного освоения теоретического материала обучающийся: знакомится со списком рекомендуемой основной и дополнительной литературы; уточняет у преподавателя, каким дополнительным пособиям следует отдать предпочтение; прорабатывает лекционный материал, пользуясь рекомендованной литературой.

На практических занятиях пройденный теоретический материал подкрепляется решением задач по основным темам дисциплины. Занятия проводятся в лаборатории, с возможностью использовать при необходимости специальное программное обеспечение. Каждой подгруппе обучающихся преподаватель выдает задачу по тематике текущего занятия. В конце занятия обучающие демонстрируют полученные результаты преподавателю и при необходимости делают работу над ошибками.

До выполнения лабораторных работ обучающийся изучает соответствующий раздел теории. Перед занятием студент знакомится с описанием заданий для выполнения работы, внимательно изучает содержание и порядок проведения лабораторной работы. Лабораторная работа проводятся в лаборатории. Обучающиеся выполняют задание на лабораторную работу. Полученные результаты исследований сводятся в отчет и защищаются по традиционной методике в классе на следующем лабораторном занятии. Необходимый теоретический материал, индивидуальное задание, шаги выполнения лабораторной работы и требование к отчету приведены в методических указаниях, размещенных на информационно-образовательном портале института.

Самостоятельная работа оказывает важное влияние на формирование личности будущего специалиста, она планируется обучающимся самостоятельно. Каждый обучающийся самостоятельно определяет режим своей работы и меру труда, затрачиваемого на овладение учебным содержанием дисциплины. Он выполняет внеаудиторную работу и изучение разделов, выносимых на самостоятельную работу, по личному индивидуальному плану, в зависимости от его подготовки, времени и других условий.

Форма заключительного контроля при промежуточной аттестации – экзамен. Для проведения промежуточной аттестации по дисциплине разработаны фонд оценочных средств и балльно-рейтинговая система оценки учебной деятельности студентов. Оценка по дисциплине выставляется в информационной системе и носит интегрированный характер, учитывающий результаты оценивания участия студентов в аудиторных занятиях, качества и своевременности выполнения заданий в ходе изучения дисциплины и промежуточной аттестации.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению *11.03.02 Инфокоммуникационные технологии и системы связи* и профилю подготовки *Интеллектуальная электроника и высокоуровневый интернет вещей*
Рабочую программу составил *д.т.н., заведующий кафедрой Дорофеев Н.В.*_____

Программа рассмотрена и одобрена на заседании кафедры *УКТС*

протокол № 37 от 16.05.2024 года.
Заведующий кафедрой *УКТС* _____*Дорофеев Н.В.*
(Подпись)

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии факультета

протокол № 9 от 17.05.2024 года.
Председатель комиссии ФИТР _____ *Рыжкова М.Н.*
(Подпись) (Ф.И.О.)

Приложение

Фонд оценочных материалов (средств) по дисциплине
Информационная безопасность и защита информации

1. Оценочные материалы для проведения текущего контроля успеваемости по дисциплине

Вопросы для тестирования размещены https://www.mivlgu.ru/iop/question/edit.php?courseid=4194

Общее распределение баллов текущего контроля по видам учебных работ для студентов

Рейтинг-контроль 1	2 практические работы, 1 лабораторная работа;	10
Рейтинг-контроль 2	4 практические работы, 2 лабораторные работы	20
Рейтинг-контроль 3	2 практические работы, 1 лабораторная работа, тестирование	10
Посещение занятий студентом		5
Дополнительные баллы (бонусы)		5
Выполнение семестрового плана самостоятельной работы		10

2. Промежуточная аттестация по дисциплине

Перечень вопросов к экзамену / зачету / зачету с оценкой.
Перечень практических задач / заданий к экзамену / зачету / зачету с оценкой (при наличии)

Вопросы для тестирования размещены https://www.mivlgu.ru/iop/question/edit.php?courseid=4194
Вопросы для подготовки к экзамену https://www.mivlgu.ru/iop/course/view.php?id=4194

Методические материалы, характеризующие процедуры оценивания

Для оценивания сформированных у студента знаний, умений и навыков имеются типовые задания. Все типовые задания разбиты на 3 блока: блок 1 - для оценивания знаний, блок 2 - для оценивания умений, блок 3 - для оценивания навыков (владений). Каждый блок включает вопросы своего уровня сложности и оценивается определенным количеством баллов. Максимальный балл, который может набрать студент при правильном ответе на все вопросы, равняется 40.

Тест для оценки знаний, умений и навыков студента состоит из 10 вопросов и формируется на основе типовых заданий программным комплексом информационно-образовательного портала МИ ВлГУ в автоматическом режими (три вопроса из блока 1, три вопроса из блока 2 и четыре вопроса из блока 3). Программный комплекс формирует индивидуальные задания для каждого зарегистрированного в системе студента и устанавливает время прохождения тестирования. Результатом тестирования является процент правильных ответов, с учетом индивидуального семестрового рейтинга студента формируется экзаменационная оценка.

При проведении устного опроса студент отвечает на выбранные случайным образом вопросы из перечня тем и в зависимости от полноты и правильности ответа с учетом индивидуального семестрового рейтинга студента формируется экзаменационная оценка.

Максимальная сумма баллов, набираемая студентом по дисциплине равна 100.

Оценка в баллах	Оценка по шкале	Обоснование	***Уровень сформированности компетенций***
Более 80	«Отлично»	Содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному	***Высокий уровень***
66-80	«Хорошо»	Содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками	***Продвинутый уровень***
50-65	«Удовлетворительно»	Содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки	***Пороговый уровень***
Менее 50	«Неудовлетворительно»	Содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки	***Компетенции не сформированы***

3. Задания в тестовой форме по дисциплине

Примеры заданий:

1. Что такое SQL-инъекция?

а) Метод ввода данных через HTML-формы

b) Тип атаки, при которой злоумышленник использует нежелательный SQL-запрос для доступа к базе данных

c) Форма атаки, при которой происходит внедрение кода в скрипты на JavaScript

d) Неопределенная ошибка в работе баз данных

Ответ: b) Тип атаки, при которой злоумышленник использует нежелательный SQL-запрос для доступа к базе данных

2. Что такое DDoS-атака?

a) Внедрение вредоносного кода через недостатки в программном обеспечении

b) Проникновение в систему для наведения шпионской деятельности

c) Атака, целью которой является насыщение сетевых ресурсов и отказ в обслуживании

d) Перехват чувствительной информации из баз данных

Ответ: c) Атака, целью которой является насыщение сетевых ресурсов и отказ в обслуживании

3. Что понимается под термином "Фишинг"?

a) Тип атаки, при котором злоумышленник создает иллюзию, что он официальный запрос от доверенной компании с целью получить личные данные

b) Несанкционированный доступ к защищенной сети

c) Взлом почтового сервера

d) Недопустимый тип аутентификации

Ответ: a) Тип атаки, при которой злоумышленник создает иллюзию, что он официальный запрос от доверенной компании с целью получить личные данные

4. Какой тип шифрования является симметричным?

a) RSA

b) AES

c) ECC

d) SHA-256

Ответ: b) AES

5. Что означает термин "безопасность периметра" (Perimeter Security)?

a) Защита сетевой инфраструктуры от внешних атак

b) Защита данных с помощью шифрования на конечных устройствах

c) Управление доступом пользователей к информации на сервере

d) Анализ сетевого трафика для обнаружения внутренних угроз

Ответ: a) Защита сетевой инфраструктуры от внешних атак

Полный перечень тестовых заданий с указанием правильных ответов, размещен в банке вопросов на информационно-образовательном портале института по ссылке https://www.mivlgu.ru/iop/question/edit.php?courseid=4194

Оценка рассчитывается как процент правильно выполненных тестовых заданий из их общего числа.