МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по УР

Документ подписан электронной подписью
Сертификат: a1119608-cdff-4455-b54e-5235117c185c
Владелец: Сенченко Павел Васильевич
Действителен: с 17.09.2019 по 16.09.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНТЕЛЛЕКТУАЛЬНОЕ ОБНАРУЖЕНИЕ ИНЦИДЕНТОВ В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ

Уровень образования: **высшее образование - магистратура**
Направление подготовки / специальность: **09.04.04 Программная инженерия**
Направленность (профиль) / специализация: **Искусственный интеллект в безопасности киберфизических систем**
Форма обучения: **очная**
Факультет: **Факультет безопасности (ФБ)**
Кафедра: **Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)**
Курс: **2**
Семестр: **3**
Учебный план набора 2023 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	3 семестр	Всего	Единицы
Лекционные занятия	20	20	часов
Лабораторные занятия	20	20	часов
Самостоятельная работа	176	176	часов
Подготовка и сдача экзамена	36	36	часов
Общая трудоемкость (включая промежуточную аттестацию)	252	252	часов
	7	7	з.е.

Формы промежуточной аттестация	Семестр
Экзамен	3

Томск

1. Общие положения

1.1. Цели дисциплины

1. Цель дисциплины "Интеллектуальное обнаружение инцидентов в киберфизических системах" заключается в формировании у студентов знаний и навыков по обнаружению и анализу инцидентов в киберфизических системах с использованием интеллектуальных методов и технологий.

1.2. Задачи дисциплины

1. Изучение основных принципов и методов обнаружения инцидентов в киберфизических системах с использованием интеллектуальных алгоритмов и технологий.
2. Освоение навыков по выбору и применению подходящих инструментов и методов для обнаружения и анализа инцидентов в киберфизических системах.
3. Приобретение практических навыков по работе с реальными данными и разработке алгоритмов для обнаружения и анализа инцидентов в киберфизических системах.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Часть блока дисциплин: Обязательная часть.
Модуль дисциплин: Модуль направления подготовки (hard skills – HS).
Индекс дисциплины: Б1.О.02.06.
Реализуется с применением электронного обучения, дистанционных образовательных технологий.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 3.1):
Таблица 3.1 – Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
Универсальные компетенции		
-	-	-
Общепрофессиональные компетенции		

ОПК-2. Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач	ОПК-2.1. Знает современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы для решения профессиональных задач	Знание перечня и содержания информационно-коммуникационных и интеллектуальных технологий, инструментальных сред для решения профессиональных задач
	ОПК-2.2. Умеет обосновывать выбор современных информационно-коммуникационных и интеллектуальных технологий, разрабатывать оригинальные программные средства для решения профессиональных задач	Демонстрация умения обосновывать выбор современных информационно-коммуникационных и интеллектуальных технологий, разрабатывать оригинальные программные средства для решения конкретных профессиональных задач
	ОПК-2.3. Владеет методами разработки оригинальных программных средств, в том числе с использованием современных информационно-коммуникационных и интеллектуальных технологий, для решения профессиональных задач	Демонстрация владения методами разработки оригинальных программных средств на примере фрагментов практической задачи

ОПК-7. Способен применять при решении профессиональных задач методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе, в глобальных компьютерных сетях	ОПК-7.1. Знает методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе, в глобальных компьютерных сетях	Знание перечня и содержания методов и средств получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе, в глобальных компьютерных сетях
	ОПК-7.2. Умеет применять методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе, в глобальных компьютерных сетях	Демонстрация умения применять методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий для решения практических задач
	ОПК-7.3. Владеет навыками, методами и средствами получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе, в глобальных компьютерных сетях	Демонстрация владения методами и средствами получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий на примере заданной предметной области
Профессиональные компетенции		
ПК-1. Способен анализировать и применять методы искусственного интеллекта и машинного обучения для защиты киберфизических систем;	ПК-1.1. Нает методы искусственного интеллекта и машинного обучения для защиты киберфизических систем	Знание перечня методов искусственного интеллекта и машинного обучения для защиты киберфизических систем, набора их основных параметров.
	ПК-1.2. Умеет использовать методы искусственного интеллекта и машинного обучения для защиты киберфизических систем	Демонстрация умения использовать методы искусственного интеллекта и машинного обучения для защиты киберфизических систем на примере практической задачи
	ПК-1.3. Владеет методами искусственного интеллекта и машинного обучения для защиты киберфизических систем	Демонстрация владения методами искусственного интеллекта и машинного обучения на примере анализа заданного набора данных

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 7 зачетных единиц, 252 академических часов.

Распределение трудоемкости дисциплины по видам учебной деятельности представлено в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины по видам учебной деятельности

Виды учебной деятельности	Всего часов	Семестры
		3 семестр

Контактная аудиторная работа обучающихся с преподавателем, всего	40	40
Лекционные занятия	20	20
Лабораторные занятия	20	20
Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего	176	176
Подготовка к тестированию	56	56
Подготовка к лабораторной работе, написание отчета	120	120
Подготовка и сдача экзамена	36	36
Общая трудоемкость (в часах)	252	252
Общая трудоемкость (в з.е.)	7	7

5. Структура и содержание дисциплины

5.1. Разделы (темы) дисциплины и виды учебной деятельности

Структура дисциплины по разделам (темам) и видам учебной деятельности приведена в таблице 5.1.

Таблица 5.1 – Разделы (темы) дисциплины и виды учебной деятельности

Названия разделов (тем) дисциплины	Лек. зан., ч	Лаб. раб.	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
3 семестр					
1 Основы обнаружения инцидентов в киберфизических системах	6	-	20	26	ОПК-2, ОПК-7, ПК-1
2 Методы и технологии обнаружения инцидентов в киберфизических системах	6	-	20	26	ОПК-2, ОПК-7, ПК-1
3 Практическое применение методов обнаружения инцидентов в киберфизических системах	8	20	136	164	ОПК-2, ОПК-7, ПК-1
Итого за семестр	20	20	176	216	
Итого	20	20	176	216	

5.2. Содержание разделов (тем) дисциплины

Содержание разделов (тем) дисциплины (в т.ч. по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов (тем) дисциплины (в т.ч. по лекциям)

Названия разделов (тем) дисциплины	Содержание разделов (тем) дисциплины (в т.ч. по лекциям)	Трудоемкость (лекционные занятия), ч	Формируемые компетенции
3 семестр			
1 Основы обнаружения инцидентов в киберфизических системах	Введение в область обнаружения инцидентов в киберфизических системах	2	ОПК-2, ОПК-7, ПК-1
	Основные понятия и принципы обнаружения инцидентов	2	ОПК-2, ОПК-7, ПК-1
	Интеллектуальные методы и технологии в обнаружении инцидентов	2	ОПК-2, ОПК-7, ПК-1
	Итого	6	

2 Методы и технологии обнаружения инцидентов в киберфизических системах	Обзор методов машинного обучения для обнаружения инцидентов	2	ОПК-2, ОПК-7, ПК-1
	Статистический анализ данных в обнаружении инцидентов	2	ОПК-2, ОПК-7, ПК-1
	Нейронные сети и глубокое обучение в обнаружении инцидентов	2	ОПК-2, ОПК-7, ПК-1
	Итого	6	
3 Практическое применение методов обнаружения инцидентов в киберфизических системах	Алгоритмы классификации для обнаружения инцидентов	2	ОПК-2, ОПК-7, ПК-1
	Алгоритмы кластеризации для обнаружения инцидентов	2	ОПК-2, ОПК-7, ПК-1
	Подготовка данных для обнаружения инцидентов	2	ОПК-2, ОПК-7, ПК-1
	Разработка и реализация алгоритмов обнаружения инцидентов	2	ОПК-2, ОПК-7, ПК-1
	Итого	8	
Итого за семестр		20	
Итого		20	

5.3. Практические занятия (семинары)

Не предусмотрено учебным планом

5.4. Лабораторные занятия

Наименование лабораторных работ приведено в таблице 5.4.

Таблица 5.4 – Наименование лабораторных работ

Названия разделов (тем) дисциплины	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
3 семестр			
3 Практическое применение методов обнаружения инцидентов в киберфизических системах	Исследование методов машинного обучения для обнаружения инцидентов в киберфизических системах	4	ОПК-2, ОПК-7, ПК-1
	Тестирование алгоритма обнаружения инцидентов на основе нейронных сетей	4	ОПК-2, ОПК-7, ПК-1
	Применение статистического анализа данных для поиска аномалий в киберфизических системах	4	ОПК-2, ОПК-7, ПК-1
	Создание и оценка модели классификации инцидентов в киберфизических системах	4	ОПК-2, ОПК-7, ПК-1
	Разработка и оптимизация алгоритма кластеризации для обнаружения схожих инцидентов в киберфизических системах	4	ОПК-2, ОПК-7, ПК-1
	Итого	20	

Итого за семестр	20	
Итого	20	

5.5. Курсовой проект / курсовая работа

Не предусмотрено учебным планом

5.6. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 5.6.

Таблица 5.6. – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов (тем) дисциплины	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
3 семестр				
1 Основы обнаружения инцидентов в киберфизических системах	Подготовка к тестированию	20	ОПК-2, ОПК-7, ПК-1	Тестирование
	Итого	20		
2 Методы и технологии обнаружения инцидентов в киберфизических системах	Подготовка к тестированию	20	ОПК-2, ОПК-7, ПК-1	Тестирование
	Итого	20		
3 Практическое применение методов обнаружения инцидентов в киберфизических системах	Подготовка к тестированию	16	ОПК-2, ОПК-7, ПК-1	Тестирование
	Подготовка к лабораторной работе, написание отчета	120	ОПК-2, ОПК-7, ПК-1	Лабораторная работа
	Итого	136		
Итого за семестр		176		
	Подготовка и сдача экзамена	36		Экзамен
Итого		212		

5.7. Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности

Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности представлено в таблице 5.7.

Таблица 5.7 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Формируемые компетенции	Виды учебной деятельности			Формы контроля
	Лек. зан.	Лаб. раб.	Сам. раб.	
ОПК-2	+	+	+	Лабораторная работа, Тестирование, Экзамен
ОПК-7	+	+	+	Лабораторная работа, Тестирование, Экзамен
ПК-1	+	+	+	Лабораторная работа, Тестирование, Экзамен

6. Рейтинговая система для оценки успеваемости обучающихся

6.1. Балльные оценки для форм контроля

Балльные оценки для форм контроля представлены в таблице 6.1.

Таблица 6.1 – Балльные оценки

Формы контроля	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
3 семестр				
Лабораторная работа	0	0	50	50
Тестирование	10	10	0	20
Экзамен				30
Итого максимум за период	10	10	50	100
Нарастающим итогом	10	20	70	100

6.2. Пересчет баллов в оценки за текущий контроль

Пересчет баллов в оценки за текущий контроль представлен в таблице 6.2.

Таблица 6.2 – Пересчет баллов в оценки за текущий контроль

Баллы на дату текущего контроля	Оценка
≥ 90% от максимальной суммы баллов на дату ТК	5
От 70% до 89% от максимальной суммы баллов на дату ТК	4
От 60% до 69% от максимальной суммы баллов на дату ТК	3
< 60% от максимальной суммы баллов на дату ТК	2

6.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 6.3.

Таблица 6.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 – 100	A (отлично)
4 (хорошо) (зачтено)	85 – 89	B (очень хорошо)
	75 – 84	C (хорошо)
	70 – 74	D (удовлетворительно)
3 (удовлетворительно) (зачтено)	65 – 69	
	60 – 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

7. Учебно-методическое и информационное обеспечение дисциплины

7.1. Основная литература

1. Системы искусственного интеллекта: Учебное пособие / Н. В. Замятин - 2018. 244 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/7269.

7.2. Дополнительная литература

1. Федеральный государственный образовательный стандарт высшего образования - магистратура по направлению подготовки 09.04.04 Программная инженерия. [Электронный ресурс]: — Режим доступа: https://workprogram3.tusur.ru/fgos/download?code=09.04.04.

7.3. Учебно-методические пособия

7.3.1. Обязательные учебно-методические пособия

1. Конев, А. А. Выявление инцидентов и противодействие атакам на объекты критической информационной инфраструктуры: учебно-методическое пособие [Электронный ресурс] / А. А. Конев, А. Ю. Якимук. — Томск: ТУСУР, 2022. — 174 с. — Режим доступа: https://edu.tusur.ru/publications/10002 [Электронный ресурс]: — Режим доступа: https://cloud.fb.tusur.ru/index.php/s/zaa2XrQKMJfpxFD.

7.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

– в форме электронного документа;

– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

– в форме электронного документа;

– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа;

– в печатной форме.

7.4. Современные профессиональные базы данных и информационные справочные системы

1. При изучении дисциплины рекомендуется обращаться к современным базам данных, информационно-справочным и поисковым системам, к которым у ТУСУРа открыт доступ: https://lib.tusur.ru/ru/resursy/bazy-dannyh.

8. Материально-техническое и программное обеспечение дисциплины

8.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с достаточным количеством посадочных мест для учебной группы, оборудованная доской и стандартной учебной мебелью. Имеются мультимедийное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

8.2. Материально-техническое и программное обеспечение для лабораторных работ

Аудитория информатики, технологий и методов программирования: учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа, помещение для курсового проектирования (выполнения курсовых работ), помещение для самостоятельной работы; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 408 ауд.

Описание имеющегося оборудования:

- Интерактивная доска IQBoard DVT TN100;
- Проектор Optoma EH400;
- Веб-камера Logitech C920s;
- Усилитель Roxton AA-60M;
- Потолочный громкоговоритель Roxton PA-20T;
- Магнитно-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- Microsoft Windows 10;
- VirtualBox;

8.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 209 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Описание имеющегося оборудования:

- учебная мебель;
- компьютеры;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду ТУСУРа.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

8.4. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися с **нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися с **нарушениями зрения** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися с **нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

9. Оценочные материалы и методические рекомендации по организации изучения дисциплины

9.1. Содержание оценочных материалов для текущего контроля и промежуточной аттестации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы, представленные в таблице 9.1.

Таблица 9.1 – Формы контроля и оценочные материалы

Названия разделов (тем) дисциплины	Формируемые компетенции	Формы контроля	Оценочные материалы (ОМ)
1 Основы обнаружения инцидентов в киберфизических системах	ОПК-2, ОПК-7, ПК-1	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов

2 Методы и технологии обнаружения инцидентов в киберфизических системах	ОПК-2, ОПК-7, ПК-1	Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов
3 Практическое применение методов обнаружения инцидентов в киберфизических системах	ОПК-2, ОПК-7, ПК-1	Лабораторная работа	Темы лабораторных работ
		Тестирование	Примерный перечень тестовых заданий
		Экзамен	Перечень экзаменационных вопросов

Шкала оценки сформированности отдельных планируемых результатов обучения по дисциплине приведена в таблице 9.2.

Таблица 9.2 – Шкала оценки сформированности планируемых результатов обучения по дисциплине

Оценка	Баллы за ОМ	Формулировка требований к степени сформированности планируемых результатов обучения		
		знать	уметь	владеть
2 (неудовлетворительно)	< 60% от максимальной суммы баллов	отсутствие знаний или фрагментарные знания	отсутствие умений или частично освоенное умение	отсутствие навыков или фрагментарные применение навыков
3 (удовлетворительно)	от 60% до 69% от максимальной суммы баллов	общие, но не структурированные знания	в целом успешно, но не систематически осуществляемое умение	в целом успешное, но не систематическое применение навыков
4 (хорошо)	от 70% до 89% от максимальной суммы баллов	сформированные, но содержащие отдельные проблемы знания	в целом успешное, но содержащие отдельные пробелы умение	в целом успешное, но содержащие отдельные пробелы применение навыков
5 (отлично)	≥ 90% от максимальной суммы баллов	сформированные систематические знания	сформированное умение	успешное и систематическое применение навыков

Шкала комплексной оценки сформированности компетенций приведена в таблице 9.3.

Таблица 9.3 – Шкала комплексной оценки сформированности компетенций

Оценка	Формулировка требований к степени компетенции
2 (неудовлетворительно)	Не имеет необходимых представлений о проверяемом материале или Знать на уровне **ориентирования**, представлений. Обучающийся знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения.

3 (удовлетворительно)	Знать и уметь на **репродуктивном** уровне. Обучающихся знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях.
4 (хорошо)	Знать, уметь, владеть на **аналитическом** уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения.
5 (отлично)	Знать, уметь, владеть на **системном** уровне. Обучающийся знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и зависимости между этим элементом и другими элементами содержания дисциплины, его значимость в содержании дисциплины.

9.1.1. Примерный перечень тестовых заданий

1. Какое из следующих утверждений верно относительно Интеллектуального обнаружения инцидентов в киберфизических системах?
   а) Это процесс, направленный на автоматизацию обнаружения и реагирования на кибератаки в реальном времени.
   б) Это технология, которая предотвращает возникновение всех инцидентов в киберфизических системах.
   в) Интеллектуальное обнаружение инцидентов в киберфизических системах не имеет никакой связи с кибербезопасностью.
   г) Это пассивный процесс, заключающийся в анализе журналов событий после возникновения инцидента.
2. Какие методы могут быть использованы для обнаружения инцидентов в киберфизических системах?
   а) Анализ журналов событий и мониторинг сетевого трафика.
   б) Использование криптографических алгоритмов.
   в) Резервное копирование данных.
   г) Профилактическая перезагрузка системы.
3. Какую роль играют алгоритмы машинного обучения в Интеллектуальном обнаружении инцидентов в киберфизических системах?
   а) Они позволяют автоматизировать обнаружение и анализ аномалий.
   б) Они осуществляют интеграцию разных систем в одну общую сеть.
   в) Алгоритмы машинного обучения не применимы в данной области.
   г) Они предоставляют администраторам возможность удаленного управления системой.
4. Какие основные принципы должны соблюдаться при разработке системы Интеллектуального обнаружения инцидентов?
   а) Проактивность и независимость от контекста.
   б) Пассивность и серийное устройство.
   в) Зависимость от контекста и исключение использования алгоритмов машинного обучения.
   г) Отсутствие анализа и реакции на инциденты.
5. Какие типы инцидентов могут быть обнаружены системой Интеллектуального обнаружения?
   а) Атаки на физическую безопасность зданий.
   б) Сбои в электропитании.
   в) Проникновения в сеть из внешней среды.
   г) Человеческий фактор.
6. Какие методы используются для анализа журналов событий в системе Интеллектуального обнаружения?
   а) Контрольный суммирования файлов.
   б) Применение алгоритмов искусственного интеллекта.

в) Интерполяция данных.
г) Построение графиков.

7. Какое из следующих утверждений верно относительно ложных срабатываний при обнаружении инцидентов?
   а) Ложные срабатывания являются нормой и их влияние на работу системы незначительно.
   б) Ложные срабатывания не возникают при использовании Интеллектуального обнаружения инцидентов.
   в) Ложные срабатывания могут снизить эффективность системы и требуют дополнительного анализа.
   г) Ложные срабатывания приводят к автоматическому выключению системы.
8. Какие действия могут быть предприняты системой Интеллектуального обнаружения после обнаружения инцидента?
   а) Автоматическое восстановление системы.
   б) Отправка уведомлений администраторам и запись события.
   в) Отключение системы от сети.
   г) Ничего, система только обнаруживает инциденты.
9. Какие характеристики являются ключевыми для системы Интеллектуального обнаружения инцидентов?
   а) Полнота и отсутствие ошибок.
   б) Точность и быстрота обнаружения.
   в) Отказоустойчивость и стабильность работы.
   г) Наличие пользовательского интерфейса.
10. Какие преимущества имеет использование Интеллектуального обнаружения инцидентов в киберфизических системах?
    а) Снижение риска кибератак и противостояние новым типам угроз.
    б) Экономия электроэнергии.
    в) Защита от физических повреждений.
    г) Автоматическая установка обновлений.

9.1.2. Перечень экзаменационных вопросов

1. Что такое интеллектуальное обнаружение инцидентов в киберфизических системах?
2. Какие основные цели преследует интеллектуальное обнаружение инцидентов в киберфизических системах?
3. Каковы основные принципы работы интеллектуальных систем обнаружения инцидентов в киберфизических системах?
4. Какие виды инцидентов в киберфизических системах могут быть обнаружены с помощью интеллектуального обнаружения?
5. Какие методы и алгоритмы используются в интеллектуальном обнаружении инцидентов в киберфизических системах?
6. Какие данные и источники информации могут быть использованы для обнаружения инцидентов в киберфизических системах?
7. Какие проблемы могут возникнуть при интеллектуальном обнаружении инцидентов в киберфизических системах?
8. Какие технические и организационные меры могут быть приняты для улучшения интеллектуального обнаружения инцидентов в киберфизических системах?
9. Каковы основные этапы процесса интеллектуального обнаружения инцидентов в киберфизических системах?
10. Как сравниваются различные методы и алгоритмы в интеллектуальном обнаружении инцидентов в киберфизических системах?
11. Каковы основные задачи, решаемые с помощью интеллектуального обнаружения инцидентов в киберфизических системах?
12. Какие компетенции и навыки необходимы для работы с интеллектуальными системами обнаружения инцидентов в киберфизических системах?
13. Каким образом может быть организована система мониторинга и управления инцидентами в киберфизических системах?
14. Каковы основные практические применения интеллектуальных систем обнаружения

инцидентов в киберфизических системах?
15. Каковы перспективы развития интеллектуального обнаружения инцидентов в киберфизических системах?

9.1.3. Темы лабораторных работ

1. Исследование методов машинного обучения для обнаружения инцидентов в киберфизических системах
2. Тестирование алгоритма обнаружения инцидентов на основе нейронных сетей
3. Применение статистического анализа данных для поиска аномалий в киберфизических системах
4. Создание и оценка модели классификации инцидентов в киберфизических системах
5. Разработка и оптимизация алгоритма кластеризации для обнаружения схожих инцидентов в киберфизических системах

9.2. Методические рекомендации

Учебный материал излагается в форме, предполагающей самостоятельное мышление студентов, самообразование. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Начать изучение дисциплины необходимо со знакомства с рабочей программой, списком учебно-методического и программного обеспечения. Самостоятельная работа студента включает работу с учебными материалами, выполнение контрольных мероприятий, предусмотренных учебным планом.

В процессе изучения дисциплины для лучшего освоения материала необходимо регулярно обращаться к рекомендуемой литературе и источникам, указанным в учебных материалах; пользоваться через кабинет студента на сайте Университета образовательными ресурсами электронно-библиотечной системы, а также общедоступными интернет-порталами, содержащими научно-популярные и специализированные материалы, посвященные различным аспектам учебной дисциплины.

При самостоятельном изучении тем следуйте рекомендациям:

– чтение или просмотр материала осуществляйте со скоростью, достаточной для индивидуального понимания и освоения материала, выделяя основные идеи; на основании изученного составить тезисы. Освоив материал, попытаться соотнести теорию с примерами из практики;

– если в тексте встречаются незнакомые или малознакомые термины, следует выяснить их значение для понимания дальнейшего материала;

– осмысливайте прочитанное и изученное, отвечайте на предложенные вопросы.

Студенты могут получать индивидуальные консультации, в т.ч. с использованием средств телекоммуникации.

По дисциплине могут проводиться дополнительные занятия, в т.ч. в форме вебинаров. Расписание вебинаров и записи вебинаров публикуются в электронном курсе / электронном журнале по дисциплине.

9.3. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 9.4.

Таблица 9.4 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы	Преимущественно письменная проверка
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)

С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами, определяющимися исходя из состояния обучающегося на момент проверки

9.4. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

– в печатной форме;
– в печатной форме с увеличенным шрифтом;
– в форме электронного документа;
– методом чтения ассистентом задания вслух;
– предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

– письменно на бумаге;
– набор ответов на компьютере;
– набор ответов с использованием услуг ассистента;
– представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:
– в форме электронного документа;
– в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:
– в форме электронного документа;
– в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:
– в форме электронного документа;
– в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

ЛИСТ СОГЛАСОВАНИЯ

Рассмотрена и одобрена на заседании кафедры КИБЭВС
протокол № 1 от «24» 1 2023 г.

СОГЛАСОВАНО:

Должность	Инициалы, фамилия	Подпись
Заведующий выпускающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d
Заведующий обеспечивающей каф. КИБЭВС	А.А. Шелупанов	Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d
И.О. начальника учебного управления	И.А. Лариошина	Согласовано, c3195437-a02f-4972-a7c6-ab6ee1f21e73

ЭКСПЕРТЫ:

Доцент, каф. КИБЭВС	А.А. Конев	Согласовано, 81687a04-85ce-4835-9e1e-9934a6085fdd
Доцент, каф. КИБЭВС	А.Ю. Якимук	Согласовано, 4ffdf265-fb78-4863-b293-f03438cb07cc

РАЗРАБОТАНО:

Доцент, каф. КИБЭВС	Е.Ю. Костюченко	Разработано, c6235dfe-234a-4234-88f9-e1597aac6463