МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета _____ Гусев П.Ю.

«31» августа 2021 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Обеспечение безопасности автоматизированных систем на основе методов искусственного интеллекта»

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация специализация N 7 "Анализ безопасности информационных систем"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2021

Автор программы _____ /Разинкин К.А./

Заведующий кафедрой Систем информационной безопасности _____ /Остапенко А.Г./

Руководитель ОПОП _____ /Остапенко А.Г./

Воронеж 2021

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины формирование представления о современном состоянии теории и практики построения интеллектуальных систем, в том числе с целью обеспечения безопасности автоматизированных систем на основе методов искусственного интеллекта

1.2. Задачи освоения дисциплины

- формирование знаний, умений и навыков в области теории и методов исследования моделей представления, хранения и обработки знаний;
- овладения умениями и навыками программирования задач обработки знаний;
- формирование системного базового представления, первичных знаний, умений и навыков студентов по основам инженерии знаний и нейроинформатике, как двум направлениям построения интеллектуальных систем;
- формирование общих представлений о прикладных системах искусственного интеллекта.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Обеспечение безопасности автоматизированных систем на основе методов искусственного интеллекта» относится к дисциплинам блока ФТД.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Обеспечение безопасности автоматизированных систем на основе методов искусственного интеллекта» направлен на формирование следующих компетенций:

ПК-7.1 - Способен применять математические модели при исследовании систем защиты информации автоматизированных систем, в том числе с использованием современных методов и программного инструментария искусственного интеллекта

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-7.1	Знать основные угрозы безопасности информации и формализует модели нарушителя в автоматизированных системах

	Уметь разрабатывать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем, в том числе с использованием современных методов и программного инструментария искусственного интеллекта

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Обеспечение безопасности автоматизированных систем на основе методов искусственного интеллекта» составляет 2 з.е.

Распределение трудоемкости дисциплины по видам занятий **очная форма обучения**

Виды учебной работы	Всего часов	Семестры
		10
Аудиторные занятия (всего)	54	54
В том числе:		
Лекции	36	36
Практические занятия (ПЗ)	18	18
Самостоятельная работа	18	18
Виды промежуточной аттестации - зачет	+	+
Общая трудоемкость: академические часы зач.ед.	72 2	72 2

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Прак зан.	СРС	Всего, час

1	*Введение в искусственный интеллект*	Определение искусственного интеллекта. Задачи искусственного интеллекта. История развития искусственного интеллекта как науки. Основные подходы к исследованию искусственного интеллекта. Основные направления исследований в области искусственного интеллекта.	6	2	2	10
2	*Введение в технологии BIG DATA*	Основы технологий больших данных. Особенности применения. Архитектуры организации систем Big Data. Big Data и Data Mining. Технологии Больших данных. Hadoop. Инфраструктура больших данных. Apache Kafka. Подход MapReduce и его программные реализации. Роль СУБД NoSQL в инфрастурктуре BigData. Apache Spark. Архитектура распределенного приложения Spark. Основные концепции Spark: RDD и DAG; основные этапы обработки данных; загрузка данных из внешнего хранилища; вычисления в Spark; Shuffle механизм; управление памятью. DataFrame API и Spark SQL.	6	2	2	10

		Создание, настройка и запуск Spark проекта. Практическое применение технологий больших данных на примерах.				

3	*Машинное обучение*	Введение: задачи обучения по прецедентам. Примеры прикладных задач. Байесовские методы классификации. Вероятностная постановка задачи классификации. Непараметрическая классификация. Нормальный дискриминантный анализ. Метрические методы классификации: метод ближайшего соседа и его обобщения. Линейные методы классификации. Аппроксимация и регуляризация эмпирического риска. Линейная модель классификации. Метод стохастического градиента. Логистическая регрессия. Метод опорных векторов. Методы восстановления регрессии. Метод наименьших квадратов. Непараметрическая регрессия: ядерное сглаживание. Линейная регрессия. Метод главных компонент. Нелинейные методы восстановления регрессии. Метод опорных векторов в задачах регрессии. Искусственные нейронные сети. Проблема полноты. Многослойные нейронные сети. Кластеризация и визуализация. Алгоритмы кластеризации. Сети Кохонена. Многомерное шкалирование. Введение в обучение с подкреплением	6	2	2	10
4	*Подходы к представлению знаний.*	Логическая модель. Продукционная модель. Фреймы. Семантические сети. Нечёткие системы и нечёткий вывод	6	4	4	14
5	*Мультиагентные системы*	Основы теории агентов и мультиагентных систем. Основные понятия. Современные подходы к решению распределенных задач. Примеры задач, решаемых посредством агентов. Общая классификация агентов. Общая характеристика мультиагентных систем. Примеры построения мультиагентных систем. Коллективное поведение агентов. Модели коллективного	6	4	4	14

		поведения. Виды моделей. Модели кооперации агентов. Конфликты в мультиагентных системах. Основные типы конфликтов. Механизмы разрешения конфликтов. Инструментарий программирования МАС.				
6	*Применение ИИ в задачах обеспечения*	Обнаружение и предотвращение вторжений. Обнаружение и изучение вредоносной активности на конечных точках: подключенных к сети рабочих станциях, серверах, устройствах Интернета вещей (EDR). *SIEM*-системы. Предотвращение утечек информации (DLP). Обнаружения и блокирования сетевых атак на веб-приложение (WAF). Поведенческий анализ действий пользователей (UEBA). Адаптивная аутентификация.	6	4	4	14
		Итого	**36**	**18**	**18**	**72**

5.2 Перечень лабораторных работ Не предусмотрено учебным планом

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе: «аттестован»;

«не аттестован».

Компе-тенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован

ПК-7.1	Знать основные угрозы безопасности информации и формализует модели нарушителя в автоматизированных системах	Знает основные угрозы безопасности информации и формализует модели нарушителя в автоматизированных системах	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь разрабатывать аналитические и	Умеет разрабатывать	Выполнение работ в срок,	Невыполнение работ в срок,
	компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем, в том числе с использованием современных методов и программного инструментария искусственного интеллекта	аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем, в том числе с использованием современных методов и программного инструментария искусственного интеллекта	предусмотренный в рабочих программах	предусмотренный в рабочих программах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 10 семестре для очной формы обучения по двухбалльной системе:

«зачтено»

«не зачтено»

Компе-тенция	**Результаты обучения, характеризующие сформированность компетенции**	**Критерии оценивания**	**Зачтено**	**Не зачтено**
ПК-7.1	Знать основные угрозы безопасности информации и формализует модели нарушителя в автоматизированных системах	Тест	Выполнение теста на 70-100%	Выполнение менее 70%

	Уметь разрабатывать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем, в том числе с использованием современных методов и программного	Решение стандартных практических задач	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	инструментария искусственного интеллекта			

7.2. Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности).

7.2.1 Примерный перечень заданий для подготовки к тестированию 1.Если произвести группировку объектов по какому-то признаку, то их можно считать…? **системой образом** структурой группой

2.Может ли в качестве образа рассматриваться группировка состояний объекта управления?

да нет

3. Что принято считать "ситуацией" в теории распознавания образов?

рассмотрения образа в структурированном виде, от высшего к низшему

уровню совокупность состояний объекта, каждое из которых характеризуется

отличительными характеристиками объекта рассмотрения образа в структурированном виде, от низшего к высшему

уровню

совокупность состояний объекта, каждое из которых характеризуется схожими характеристиками объекта

4. В распознавании образов сначала следует распознавание, а потом обучение?

нет да

5.В чем состоит проблема распознавания образов?

в обучении **в**

распознавании

6.Что является результатом обучения?

появление разных реакций на все объекты одного образа **появление**

одинаковых реакций на все объекты одного образа

формировании базы данных объектов

7. Процесс обучения должен завершиться путем показа…?

конечного числа объектов дополнительными

подсказками

конечного числа объектов и дополнительными подсказками 8.

Что представляет собой анализ образов?

процесс расчленения образа верхнего уровня, на объекты, принадлежащие низшим уровням процесс объединения образов низшего уровня, в образ, принадлежащий

верхнему уровню процесс выделения из совокупности образов наиболее схожих

изображений

9. Можно ли считать множество изображений, объединенных разными свойствами, образом?

да **нет**

10.Какое из нижеследующих понятий является аналогом понятия "образ"?

ситуация состояния

изображение

11. Одной из центральных задач проблемы ОРО является?

выбор исходного описания объектов интерпретация полученных результатов автоматизация процесса распознавания образов

12. Последовательность ситуаций с указанием, к какому классу они относятся, называется?

последовательность обучения

последовательность образов **обучающая**

последовательность

последовательность изображений

7.2.2 Примерный перечень заданий для решения стандартных задач 1. Самым известным среди эволюционных алгоритмов является ... **генетический алгоритм** метод группового учета аргументов алгоритм поиска глобального экстремума алгоритм конкурирующих точек

2. Какой генетический оператор наиболее важный:

мутация **кроссовер** инверсия

3. Что является ключевой эвристикой всех

эволюционных методов? перебор всех объектов **отбор**

наилучших объектов отсечение ложных объектов

4.Сколько может иметь поддеревьев каждый из узлов бинарного дерева?

1

2 +

3

4

5. Любой элемент в правой части бинарного дерева должен быть ….

корня меньше **больше**

равен не имеет

значения

6. Любой элемент в левой части бинарного дерева должен быть ….

корня **меньше**

больше

равен

не имеет значения

7. Физический принцип действия (ФПД) - это ориентированный граф, вершинами которого являются физические объекты В, а ребрами входные А и выходные С потоки?

да +

нет

8. На какой модели базируется описание технической функции?

на модели "черный ящик" на

структурированной модели на

организационной модели 9. Сколько

уровней описания имеет ФТЭ?

1

2

3 +

4

10. На первом уровне описания ФТЭ приводится следующая информация:

стандартная карта описания ФТЭ **самое**

короткое качественное описание ФТЭ более

подробное описание ФТЭ

11. Что служит основой логического подхода построения систем искусственного интеллекта?

логика **булева**

алгебра +

тригонометрия

теория вероятности

12. Что представляет собой система искусственного интеллекта, построенная на логическом принципе?

машину доказательства теорем + программу

вычисления значений по формулам систему решения

простых алгебраических вычислений программу

решения тригонометрических задач

13. Чем определяется мощность системы искусственного интеллекта, построенная на логическом принципе?

скоростью обработки транзакций

возможностями генератора целей +

машиной доказательства теорем +

качеством полученных результатов

14. Где хранятся исходные данные системы искусственного интеллекта, построенной на логическом принципе и в виде чего?

на листке бумаге и в виде записей

в таблице excel и в виде закодированных правил **в**

базе данных и в виде аксиом

15. Что позволило логическому подходу придать большей выразительности?

нечеткая логика теория

вероятности логика

предикатов

математическая статистика

7.2.3 Примерный перечень заданий для решения прикладных задач

1. Как выглядит бинарный линейный классификатор? (Формула для отображения из множества объектов в множество классов.)

2. Что такое отступ алгоритма на объекте? Какие выводы можно сделать из знака отступа?

3. Как классификаторы вида $a\ x(\ )\ \square\ sign(\square\ w\ x,\ \square\square w_0)$ сводят к классификаторам вида $a(x) = sign(< w, x >)$?

4. Как выглядит запись функционала эмпирического риска через отступы? Какое значение он должен принимать для «наилучшего» алгоритма классификации?

5. Если в функционале эмпирического риска всюду написаны строгие неравенства ($M_i < 0$) можете ли вы сразу придумать параметр w для алгоритма классификации $a(x) = sign(< w, x >)$, минимизирующий такой функционал?

6. Запишите функционал аппроксимированного эмпирического риска, если выбрана функция потерь $L(M)$.

7. Что такое функция потерь, зачем она нужна? Как обычно выглядит ее график?

8. В чем практический смысл квадратичной функции потерь? Почему может быть полезна функция потерь, принимающая большие значения для большого положительного отступа?

9. Приведите пример негладких и немонотонный функций потерь.

10. Что такое регуляризация? Какие регуляризаторы вы знаете?

11. Как связаны переобучение и обобщающая способность алгоритма. Как влияет регуляризация на обобщающую способность?

12. Как связаны острые минимумы функционала аппроксимированного эмпирического риска с проблемой переобучения?

13. Что делает регуляризация с аппроксимированным риском как функцией параметров алгоритма?

14. Для какого алгоритма классификации функционал аппроксимированного риска будет принимать большее значение на обучающей выборке: для построенного с регуляризацией или без нее? Почему?

15. Что представляют собой метрики качества Accuracy, Precision и Recall?

7.2.4 Примерный перечень вопросов для подготовки к зачету

Определение искусственного интеллекта. Задачи искусственного интеллекта. История развития искусственного интеллекта как науки. Основные подходы к исследованию искусственного интеллекта. Основные

направления исследований в области искусственного интеллекта. Основы технологий больших данных. Особенности применения. Архитектуры организации систем Big Data. Big Data и Data Mining. Технологии Больших данных. Hadoop. Инфраструктура больших данных. Apache Kafka. Подход MapReduce и его программные реализации. Роль СУБД NoSQL в инфрастурктуре BigData. Apache Spark. Архитектура распределенного приложения Spark. Основные концепции Spark: RDD и DAG; основные этапы обработки данных; загрузка данных из внешнего хранилища; вычисления в Spark; Shuffle механизм; управление памятью. DataFrame API и Spark SQL. Создание, настройка и запуск Spark проекта. Практическое применение технологий больших данных на примерах.

Введение: задачи обучения по прецедентам. Примеры прикладных задач.

Байесовские методы классификации. Вероятностная постановка задачи классификации. Непараметрическая классификация. Нормальный дискриминантный анализ.

Метрические методы классификации: метод ближайшего соседа и его обобщения.

Линейные методы классификации. Аппроксимация и регуляризация эмпирического риска. Линейная модель классификации. Метод стохастического градиента. Логистическая регрессия. Метод опорных векторов. Методы восстановления регрессии. Метод наименьших квадратов. Непараметрическая регрессия: ядерное сглаживание. Линейная регрессия. Метод главных компонент. Нелинейные методы восстановления регрессии. Метод опорных векторов в задачах регрессии. Искусственные нейронные сети. Проблема полноты. Многослойные нейронные сети. Кластеризация и визуализация. Алгоритмы кластеризации. Сети Кохонена. Многомерное шкалирование. Введение в обучение с подкреплением

Логическая модель. Продукционная модель. Фреймы. Семантические сети. Нечёткие системы и нечёткий вывод

Основы теории агентов и мультиагентных систем. Основные понятия. Современные подходы к решению распределенных задач. Примеры задач, решаемых посредством агентов. Общая классификация агентов.

Общая характеристика мультиагентных систем. Примеры построения мультиагентных систем. Коллективное поведение агентов. Модели коллективного поведения. Виды моделей. Модели кооперации агентов. Конфликты в мультиагентных системах. Основные типы конфликтов.
Механизмы разрешения конфликтов. Инструментарий программирования MAC.

Обнаружение и предотвращение вторжений. Обнаружение и изучение вредоносной активности на конечных точках: подключенных к сети рабочих станциях, серверах, устройствах Интернета вещей (EDR). SIEM-системы. Предотвращение утечек информации (DLP). Обнаружения и блокирования сетевых атак на веб-приложение (WAF). Поведенческий анализ действий пользователей (UEBA). Адаптивная аутентификация.

7.2.5 Примерный перечень заданий для решения прикладных задач

Не предусмотрено учебным планом

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

(Например: Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.)

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Введение в искусственный интеллект	ПК-7.1	Тест, защита практических работ
2	Введение в технологии BIG DATA	ПК-7.1	Тест, защита практических работ
3	Машинное обучение	ПК-7.1	Тест, защита практических работ
4	Подходы к представлению знаний.	ПК-7.1	Тест, защита практических работ
5	Мультиагентные системы	ПК-7.1	Тест, защита практических работ
6	Применение ИИ в задачах обеспечения	ПК-7.1	Тест, защита практических работ

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная литература

Гаврилова, И. В. Основы искусственного интеллекта : учебное пособие / И. В. Гаврилова, О. Е. Масленникова. — 3-е изд., стер. — Москва : ФЛИНТА, 2019. — 283 с. — ISBN 978-5-9765-1602-1. — Текст : электронный // Лань :
электронно-библиотечная система. — URL: https://e.lanbook.com/book/115839

Боровская, Е.В. Основы искусственного интеллекта : учебное поң собие / Е. В. Боровская, Н. А. Давыдова. Ч 4ңе изд., электрон. Ч М. : Лаборатория знаний, 2020. Ч 130 с. - Текст : электронный // URL: https://www.rulit.me/data/programs/resources/pdf/Osnovy-iskusstvennogo-intellekta_RuLit_Me_643478.pdf Воронцов, К.В. Машинное обучение: курс лекций - Текст : электронный. — URL:

http://www.machinelearning.ru/wiki/index.php?title=%D0%9C%D0%B0%D1%88%D0%B8%D0%BD%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D1%83%D1%87%D0%B5%D0%BD%D0%B8%D0%B5_%28%D0%BA%D1%83%D1%80%D1%81_%D0%BB%D0%B5%D0%BA%D1%86%D0%B8%D0%B9%2C_%D0%9A.%D0%92.%D0%92%D0%BE%D1%80%D0%BE%D0%BD%D1%86%D0%BE%D0%B2%29

Дополнительная литература

Романов, П. С. Системы искусственного интеллекта. Моделирование нейронных сетей в системе MATLAB. Лабораторный практикум : учебное пособие для вузов / П. С. Романов, И. П. Романова. — Санкт-Петербург : Лань, 2021. — 140 с. — ISBN 978-5-8114-7747-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/179031

Воронов, М. В. Системы искусственного интеллекта : учебник и практикум для вузов / М. В. Воронов, В. И. Пименов, И. А. Небаев. — Москва : Издательство Юрайт, 2022. — 256 с. — (Высшее образование). — ISBN 978-5-534-14916-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/485440

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

Банк данных угроз безопасности информации. Электрон. дан. - Режим доступа: http://www.bdu.fstec.ru

Стандарт Common Vulnerabilities and Exposures. Электрон. дан. - Режим доступа: http://cve.mitre.org

База данных с информационными бюллетенями (Secunia Advisories), содержащими сведения об обнаруженных угрозах и уязвимостях ПО Secunia Advisory and Vulnerability Database Электрон. дан. - Режим доступа: https://secuniaresearch.flexerasoftware.com/community/advisories

База уязвимостей VND (Vulnerability Notes Database Электрон. дан. - Режим доступа: https://www.kb.cert.org/vuls

База сценариев эксплуатации уязвимостей Exploit Database Электрон. дан. - Режим доступа: https://www.exploit-db.com

Агрегатор информации об уязвимостях CVEDetails. Электрон. дан. - Режим доступа: https://www.cvedetails.com

Information Security Информационная безопасность. Электрон. дан. - Режим доступа: http://www.itsec.ru

Securitylab.ru by Positive Technologies. Электрон. дан. - Режим доступа: https://www.securitylab.ru/

Anti-Malware.ru. Электрон. дан. - Режим доступа: https://www.anti-malware.ru/news

Iso27000.ru Искусство управления информационной безопасностью. Электрон. дан. - Режим доступа: http://www.iso27000.ru/

SecurityPolicy.ru Документы по информационной безопасности. Электрон. дан. - Режим доступа: http://securitypolicy.ru/

SearchInform – Информационная безопасность. Электрон. дан. - Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/

Информационная безопасность предприятия. Электрон. дан. - Режим доступа: Ekrost.ru

http://att.nica.ru http://www.edu.ru/

http://window.edu.ru/window/library http://www.intuit.ru/catalog/

http://bibl.cchgeu.ru/MarcWeb2/ExtSearch.asp

https://cchgeu.ru/education/cafedras/kafsib/?docs

http://www.eios.vorstu.ru

http://e.lanbook.com/ (ЭБС Лань)

http://IPRbookshop.ru/ (ЭБСIPRbooks)

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой

Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Обеспечение безопасности автоматизированных систем на основе методов искусственного интеллекта» читаются лекции, проводятся практические занятия.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Практические занятия направлены на приобретение практических навыков:

1. Использование Apache Spark MLlib для создания приложения машинного обучения и анализа набора данных
2. Байесовские методы классификации/
3. Метрические методы классификации.
4. Линейная регрессия. Метод главных компонент.
5. Модели коллективного поведения.
6. SIEM-системы ориентированные на модели и методы ИИ и машинного обучения.

Занятия проводятся путем решения конкретных задач в аудитории.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.

Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом три дня эффективнее всего использовать для повторения и систематизации материала.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Перечень вносимых изменений	Дата извнмеесненеенниия й	Подпись заведующего кафедрой, ответственной за реализацию ОПОП
1	2	3	4
