Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет имени В.А. Бондаренко»

Кафедра вычислительной техники и защиты информации

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.Б.41 Системы искусственного интеллекта в задачах защиты информации»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
10.03.01 Информационная безопасность
(код и наименование направления подготовки)

Безопасность автоматизированных систем (информационные технологии и электронная промышленность)
(наименование направленности (профиля) образовательной программы)

Квалификация
Бакалавр

Форма обучения
Очная

Год набора 2026

Рабочая программа дисциплины «*Б1.Д.Б.41 Системы искусственного интеллекта в задачах защиты информации*» рассмотрена и утверждена на заседании кафедры

Кафедра вычислительной техники и защиты информации
наименование кафедры

протокол № 10 от 10 марта 2025 г.

Заведующий кафедрой
Кафедра вычислительной техники и защиты информации — В.В. Тугов
наименование кафедры — подпись — расшифровка подписи

Исполнители:
доцент кафедры ВТиЗИ — Р.Р. Галимов
должность — подпись — расшифровка подписи

должность — подпись — расшифровка подписи

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
10.03.01 Информационная безопасность — В.В. Тугов
код наименование — личная подпись — расшифровка подписи

Заведующий отделом формирования фонда и научной обработки документов
Главный библиограф — Г.Г. Гасанбегова
личная подпись — расшифровка подписи

Уполномоченный по качеству факультета
С.Н. Морозова
личная подпись — расшифровка подписи

№ регистрации _____

© Галимов Р.Р., 2026
© ОГУ, 2026

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины: сформировать у студентов базовые знания и практические навыки применения базовых методов искусственного интеллекта для решения типовых задач защиты информации (обнаружение аномалий, классификация угроз, поддержка принятия решений).

Задачи:

– изучить основные понятия и методы ИИ применительно к информационной безопасности;

– научиться обрабатывать и анализировать данные о сетевом трафике и событиях безопасности с использованием открытых инструментов;

– освоить построение моделей обнаружения аномалий, классификации атак и прогнозирования рисков;

– получить навыки работы с бесплатными библиотеками машинного обучения и открытыми наборами данных.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.В.1 Прикладная теория алгоритмов и математической логики в вычислительной технике*

Постреквизиты дисциплины: *Отсутствуют*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1-В-1 Применяет философские основы познания и логического мышления, методы научного познания, в том числе методы системного анализа, для решения поставленных задач УК-1-В-2 Осуществляет критический анализ и синтез информации, полученной из разных источников УК-1-В-3 Понимает основные закономерности и главные особенности социально-исторического развития различных культур в этическом и философском контексте УК-1-В-4 Применяет методы сбора, хранения, обработки, передачи, анализа и синтеза информации с использованием компьютерных технологий для решения поставленных задач УК-1-В-5 Формулирует и аргументирует выводы и суждения, в том числе с применением философского понятийного	**Знать:** основные методы сбора, хранения, обработки, передачи, анализа и синтеза информации с использованием компьютерных технологий. **Уметь:** - применять системный подход и методы логического мышления для решения задач защиты автоматизированных систем с использованием методов искусственного интеллекта; - осуществлять критический анализ и синтез информации, полученной из разных

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
	аппарата УК-1-В-6 Формулирует собственную гражданскую и мировоззренческую позицию с опорой на системный анализ философских взглядов и исторических закономерностей, процессов, явлений и событий	источников, формулировать и аргументировать выводы и суждения. **Владеть:** - навыками применения методов системного анализа, сбора, хранения, обработки и синтеза информации с использованием компьютерных технологий для решения практических задач защиты информации; -навыками критической оценки информации, аргументации выводов и представления результатов интеллектуального анализа данных в профессиональной и междисциплинарной коммуникации
ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-8-В-1 Выполняет аналитический обзор, подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности ОПК-8-В-2 Умеет осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения профессиональных задач	**Знать:** - основные источники научно-технической литературы, нормативных и методических документов в области искусственного интеллекта и информационной безопасности; -принципы систематизации, анализа и обобщения научно-технической информации применительно к задачам построения интеллектуальных систем защиты информации. **Уметь:** Осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов для обоснования выбора

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		методов и средств искусственного интеллекта в задачах защиты автоматизированных систем. **Владеть:** навыками обобщения изученной литературы для подготовки отчётов по лабораторным работам, презентаций и защиты решений, используя корректные ссылки на источники и соблюдая требования академической этики

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 академических часов).

Вид работы	Трудоемкость, академических часов	
	7 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**68,25**	**68,25**
Лекции (Л)	34	34
Лабораторные работы (ЛР)	34	34
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- выполнение индивидуального творческого задания (ИТЗ);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- изучение разделов курса в системе электронного обучения;* *- подготовка к лабораторным занятиям;* *- подготовка к рубежному контролю)*	**39,75**	**39,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**диф. зач.**	

Разделы дисциплины, изучаемые в 7 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Введение в ИИ и задачи ИБ	26	4		2	20

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
2	Использование ИИ для обнаружения угроз в АС	28	10		12	6
3	Прогнозирование состояния защищенности АС	26	10		8	8
4	Принятие решений по нейтрализации угроз в АС	28	10		12	6
	Итого:	108	34		34	40
	Всего:	108	34		34	40

4.2 Содержание разделов дисциплины

1. Введение. Основные понятия искусственного интеллекта (ИИ) применительно к защите информации. Классификация задач ИБ, решаемых методами ИИ: -обнаружение аномалий и вторжений; -классификация вредоносного ПО; - прогнозирование уязвимостей и рисков; -поддержка принятия решений при реагировании на инциденты. Обзор открытых наборов данных для задач ИБ. Обзор свободного программного обеспечения для машинного обучения. Этические аспекты применения ИИ в ИБ (приватность, возможное использование злоумышленниками).

2. Использование ИИ для обнаружения угроз в автоматизированных системах (АС). Признаки сетевых атак (длительность, количество байт, количество SYN-пакетов и т.п.) и их отражение в наборах данных. Метод дерева решений. Метод K-средних для кластеризации трафика. Оценка качества моделей обнаружения: матрица ошибок, точность, полнота, F1-мера, ROC-кривая и AUC для бинарной классификации.

3. Прогнозирование состояния защищённости автоматизированных систем (АС). Задачи прогнозирования в ИБ: предсказание вероятности атаки, динамики уязвимостей, уровня защищённости.2 Методы прогнозирования на основе временных рядов: скользящее среднее, экспоненциальное сглаживание; подходы машинного обучения (линейная регрессия, деревья решений). Оценка защищённости с помощью правил и нечёткой логики (введение). Проблема ограниченных данных и способы её смягчения.

4. Принятие решений по нейтрализации угроз в автоматизированных системах (АС). Структура задач принятия решений в системах защиты: выбор типа реакции (блокировка, оповещение, анализ), назначение строгости политик. Нечёткая логика для принятия решений в условиях неопределённости: лингвистические переменные, функции принадлежности; база правил; дефаззификация. Экспертные системы (простые продукционные модели): представление знаний в виде правил «ЕСЛИ-ТО»; механизм прямого вывода. Генетические алгоритмы для оптимизации параметров защиты (порогов срабатывания, весов).

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Знакомство с набором данных и первичный анализ	2
2	2	Классификация атак с помощью дерева решений	4
3	2	Обнаружение аномалий методом K-means	4
4	2	Сравнение дерева решений и K-means	4
5	3	Прогнозирование количества атак с помощью линейной регрессии	4
6	3	Классификация уровня защищённости компонента АС	4
7	4	Нечёткая система для управления межсетевым экраном	6
8	4	Генетический алгоритм для оптимизации порога детектора аномалий	6
		Итого:	34

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Платонов, В. В. Технологии машинного обучения в кибербезопасности : учебное пособие / В. В. Платонов. – Москва ; Вологда : Инфра-Инженерия, 2024. – 140 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=725700 (дата обращения: 05.05.2026). – Библиогр. в кн. – ISBN 978-5-9729-2048-8. – Текст : электронный.

2. Целых, А. Н. Выявление инцидентов информационной безопасности и мошеннических транзакций методами машинного обучения : учебное пособие : [16+] / А. Н. Целых, Э. М. Котов ; Южный федеральный университет, Южный федеральный университет, Инженерно-технологическая академия. – Ростов-на-Дону : Южный федеральный университет, 2023. – 118 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=713464 (дата обращения: 05.05.2026). – Библиогр. в кн. – ISBN 978-5-9275-4515-5. – Текст : электронный.

5.2 Дополнительная литература

1. Подоплелова, Е. С. Современные методы инженерии знаний в задачах машинного обучения : учебное пособие : [16+] / Е. С. Подоплелова ; Южный федеральный университет, Инженерно-технологическая академия. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2025. – 130 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=724468 (дата обращения: 05.05.2026). – Библиогр. в кн. – ISBN 978-5-9275-4882-8. – Текст : электронный.

2. Целых, А. Н. Применение алгоритмов машинного обучения в прикладных задачах : учебное пособие : [16+] / А. Н. Целых, Э. М. Котов ; Южный федеральный университет, Инженерно-технологическая академия. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2025. – 126 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=732067 (дата обращения: 05.05.2026). – Библиогр. в кн. – ISBN 978-5-9275-5103-3. – Текст : электронный.

5.3 Периодические издания

1. Автоматизация процессов управления = Automation of Control Processes / гл. ред. В. А. Маклаев ; учред. и изд. Научно-производственное объединение «Марс». – Ульяновск : Научно-производственное объединение «Марс», 2023-2025 – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=732128. – ISSN 1991-2927. – Текст : электронный.

2. Прикладная информатика / гл. ред. М. И. Дли ; учред. и изд. Университет «Синергия». – Москва : Университет Синергия, 2024 - 2025. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=719829. – ISSN 1993-8314 (Print). – ISSN 2687-0649 (Online). – DOI 10.37791/2687-0649-2024-19-4. – Текст : электронный.

5.4 Интернет-ресурсы

1. Основы теории нечетких множеств. https://intuit.ru/studies/courses/87/87/info
2. Искусственный интеллект в киберзащите. https://stepik.org/course/233239

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система РЕД ОС.
2. Пакет офисных приложений «МойОфис Образование»
3. Для работы с ресурсами Интернет - веб-браузер Яндекс https://yandex.ru/..
4. ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990–2026]. – Режим доступа в сети ОГУ http://garant.net.osu.ru
5. Автоматизированная интерактивная система сетевого тестирования - АИССТ (зарегистрирована в РОСПАТЕНТ, Свидетельство о государственной регистрации программы для ЭВМ №2011610456, правообладатель – Оренбургский государственный университет), режим доступа - http://aist.osu.ru.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения лабораторных занятий используется лаборатория компьютерный класс.

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к сети "Интернет", и обеспечением доступа в электронную информационно-образовательную среду ОГУ.