Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» (ВлГУ)

Институт информационных технологий и радиоэлектроники

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Искусственный интеллект для информационной безопасности»

направление подготовки / специальность
09.04.01 «Информатика и вычислительная техника»

направленность (профиль) подготовки
Инженерия искусственного интеллекта

г. Владимир
2022

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью дисциплины «Искусственный интеллект для информационной безопасности» является изучение возможных путей использования искусственного интеллекта в области обеспечения информационной безопасности. Формирование умений по использованию технологий искусственного интеллекта для предотвращения несанкционированного доступа к информации, а также уменьшения последствий при нарушении информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Искусственный интеллект для информационной безопасности» относится к части учебного плана, формируемой участниками образовательных отношений.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесённые 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 *(код, содержание индикатора*	Результаты обучения по дисциплине	
УК-7 Способен понимать фундаментальные принципы работы современных систем искусственного интеллекта, разрабатывать правила и стандарты взаимодействия человека и искусственного интеллекта и использовать их в социальной и профессиональной деятельности.	УК-7.1. Знает нормативно-правовую базу, правовые, этические правила, стандарты при решении задач искусственного интеллекта. УК-7.2. Умеет применять нормативно-правовую базу, правовые, этические правила, стандарты при решении задач искусственного интеллекта УК-7.3. Владеет современными методами и инструментами для представления результатов научно-исследовательской деятельности	Делает обзор угроз информационной безопасности, основных принципов организации безопасной работы в информационных системах и в сети интернет. Описывает способы и средства защиты персональных данных и данных в организации в соответствии с действующим законодательством. Определяет основные угрозы безопасности при использовании информационных технологий и выбирает оптимальные способы и средства защиты. Обосновывает выбор технических и программных средств защиты персональных данных и данных организации при работе с информационными системами на основе анализа потенциальных и реальных угроз безопасности информации. Решает поставленные задачи, используя эффективные цифровые средства и средства информационной	вопросы для рейтинг-контроля, задания для самостоятельной работы, вопросы зачета

		безопасности.	
ПК-8. Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учётом требований информационной безопасности в различных предметных областях.	ОПК-8.1. Знать: методологии эффективного управления разработкой программных средств и проектов. ОПК-8.2. Уметь: планировать комплекс мероприятий по разработке программных средств и проектов. ОПК-8.3. Иметь навыки: разработки программных средств и проектов в команде.	Знает новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях. Умеет разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учётом требований информационной безопасности для решения профессиональных задач в различных предметных областях	вопросы для рейтинг-контроля, задания для самостоятельной работы, вопросы зачета

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов

Тематический план
форма обучения – очная

№ п/п	Наименование тем и/или разделов/тем дисциплины	Семестр	Неделя семестра	Контактная работа обучающихся с педагогическим работником				Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	*в форме практической подготовки*		
1	Основы компьютерной безопасности	2	1-6	6	6		4	12	Рейтинг-контроль №1
2	Применение машинного обучения для задач информационной безопасности	2	7-12	6	6		4	12	Рейтинг-контроль №2
3	Проекты искусственного интеллекта в области информационной безопасности	2	13-18	6	6		4	12	Рейтинг-контроль №3
Всего за 3 семестр:				18	18			72	Зачет
Наличие в дисциплине КП/КР									
Итого по дисциплине				18	18			72	Зачет

Содержание лекционных занятий по дисциплине

1. Основы компьютерной безопасности

Типы атак в информационной безопасности.
Криптография.
Хэш-функции.
Безопасность компьютерных сетей и сетевых протоколов.
Безопасность в ОС Linux.
Инъекции.
Бинарные уязвимости.

2. Применение машинного обучения для задач информационной безопасности

Определение спама.
Классификация сетевых атак.
Определение распределённой сетевой атаки “отказ в обслуживании”.
Определение злонамеренных (malicious) сайтов.
Определение инъекций.
Поиск злонамеренного программного обеспечения (malware).
Анализ аномалий в активности пользователей.

3. Проекты искусственного интеллекта в области информационной безопасности

Жизненный цикл проекта создания приложений искусственного интеллекта для информационной безопасности.
Подготовка набора данных в информационной безопасности.
Выбор модели и её обучение.
Оценка качества модели.
Разработка приложения, использующего модель.
Внедрение приложения в практическое использование.

Содержание практических занятий по дисциплине

1. Модели атак в информационной безопасности.
2. Решение задач информационной безопасности с использованием классификации.
3. Решение задач информационное безопасности с использованием кластеризации.
4. Решение задач информационной безопасности с использованием определения аномалий.
5. Решение задач информационной безопасности с использованием состязательного машинного обучения.
6. Определение спама с помощью методов машинного обучения.
7. Злонамеренное программное обеспечение и его определение с помощью методов машинного обучения.
8. Злонамеренные сайты и их определение с помощью методов машинного обучения.
9. Анализ сетевого трафика с помощью методов машинного обучения.
10. Обнаружение сетевых вторжений с помощью методов машинного обучения.
11. Обнаружение распределённых сетевых атак с помощью методов машинного обучения.
12. Обнаружение аномалий в активности пользователей с помощью методов машинного обучения.
13. Обнаружение SQL-инъекций с помощью методов машинного обучения.
14. Жизненный цикл проекта создания приложений искусственного интеллекта для информационной безопасности.

15. Подготовка набора данных для систем искусственного интеллекта для информационной безопасности. Качество данных. Очистка данных.

16 Поиск злонамеренного программного обеспечения.

17. Выбор модели машинного обучения для систем искусственного интеллекта для информационной безопасности.

18. Оценка качества систем искусственного интеллекта для информационной безопасности.

Содержание самостоятельной работы

Задания в составе контрольных работ:

1. Атака “отказ в обслуживании”.
2. Атака “распределенный отказ в обслуживании”.
3. Атака “человек посередине”.
4. Атака “SQL-инъекции”.
5. Атака “переполнение буфера”.
6. Неавторизованный доступ.
7. Получение привилегий администратора.
8. Злонамеренное программное обеспечение.
9. Злонамеренные сайты.

Домашняя работа

Примерная тематика домашних работ*:*

Домашняя работа №1:

Определение сетевых атак.

Домашняя работа №2:

Обнаружение злонамеренных сайтов.

Примерные задания в составе домашних работ***:***

1. Используя набор данных о сетевых атаках KDD Cup 1999 (http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html) обучите модель машинного обучения находить сетевые атаки и определять их тип. Точность работы модели необходимо измерять на тестовом наборе данных KDD Cup 1999.

2. Создайте и обучите модель модель машинного обучения для определения злонамеренных сайтов. Для обучения используйте набор данных Malicious and Benign Websites – https://www.kaggle.com/x

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

5.1. Текущий контроль успеваемости

Рейтинг-контроль №1

1. Модели атак в информационной безопасности.
2. Решение задач информационной безопасности с использованием классификации.
3. Решение задач информационное безопасности с использованием кластеризации.
4. Решение задач информационной безопасности с использованием определения аномалий.
5. Решение задач информационной безопасности с использованием состязательного машинного обучения.

6. Определение спама с помощью методов машинного обучения.

Рейтинг-контроль №2

1 Злонамеренное программное обеспечение и его определение с помощью методов машинного обучения.
2 Злонамеренные сайты и их определение с помощью методов машинного обучения.
3 Анализ сетевого трафика с помощью методов машинного обучения.
4 Обнаружение сетевых вторжений с помощью методов машинного обучения.
5 Обнаружение распределенных сетевых атак с помощью методов машинного обучения.
6 Обнаружение аномалий в активности пользователей с помощью методов машинного обучения.

Рейтинг-контроль №3

1. Обнаружение SQL-инъекций с помощью методов машинного обучения.
2. Жизненный цикл проекта создания приложений искусственного интеллекта для информационной безопасности.
3. Подготовка набора данных для систем искусственного интеллекта для информационной безопасности. Качество данных. Очистка данных.
4. Поиск злонамеренного программного обеспечения.
5. Выбор модели машинного обучения для систем искусственного интеллекта для информационной безопасности.
6. Оценка качества систем искусственного интеллекта для информационной безопасности.

5.2. Промежуточная аттестация по итогам освоения дисциплины *(зачёт)*

Вопросы к зачёту:

1. Модели атак в информационной безопасности.
2. Решение задач информационной безопасности с использованием классификации.
3. Решение задач информационной безопасности с использованием кластеризации.
4. Решение задач информационной безопасности с использованием определения аномалий.
5. Решение задач информационной безопасности с использованием состязательного машинного обучения.
6. Определение спама с помощью методов машинного обучения.
7. Злонамеренное программное обеспечение и его определение с помощью методов машинного обучения.
8. Злонамеренные сайты и их определение с помощью методов машинного обучения.
9. Анализ сетевого трафика с помощью методов машинного обучения.
10. Обнаружение сетевых вторжений с помощью методов машинного обучения.
11. Обнаружение распределённых сетевых атак с помощью методов машинного обучения.
12. Обнаружение аномалий в активности пользователей с помощью методов машинного обучения.
13. Обнаружение SQL-инъекций с помощью методов машинного обучения.
14. Жизненный цикл проекта создания приложений искусственного интеллекта для информационной безопасности.
15. Подготовка набора данных для систем искусственного интеллекта для информационной безопасности. Качество данных. Очистка данных.
16. Формирование признаков для для систем искусственного интеллекта для информационной безопасности.

17. Выбор модели машинного обучения для систем искусственного интеллекта для информационной безопасности.
18. Оценка качества систем искусственного интеллекта для информационной безопасности.
19. Разработка приложений искусственного интеллекта для информационной безопасности.
20. Открытое программное обеспечение для информационной безопасности. Интеграция с системами искусственного интеллекта.

5.2.1 Зачёт проводится в традиционной форме (устные /письменные ответы на вопросы) согласно списка предложенных вопросов.

5.3. Самостоятельная работа обучающегося

Самостоятельная работа обучающихся заключается в самостоятельном изучении отдельных тем, практической реализации заданий самостоятельной работы по этим темам, выполнении контрольных работ. Контроль выполнения самостоятельной работы проводится при текущих контрольных мероприятиях и на промежуточной аттестации по итогам освоения дисциплины. Учебно-методическое обеспечение самостоятельной работы – основная литература [1-3], дополнительная литература [1-2].

Примерные задания в составе контрольных работ:

1. Атака “отказ в обслуживании”.
2. Атака “распределенный отказ в обслуживании”.
3. Атака “человек посередине”.
4. Атака “SQL-инъекции”.
5. Атака “переполнение буфера”.
6. Неавторизованный доступ.
7. Получение привилегий администратора.
8. Злонамеренное программное обеспечение.
9. Злонамеренные сайты.

5.1.5. Домашняя работа

Примерная тематика домашних работ***:***

Домашняя работа №1:

Определение сетевых атак.

Домашняя работа №2:

Обнаружение злонамеренных сайтов.

Примерные задания в составе домашних работ***:***

1. Используя набор данных о сетевых атаках KDD Cup 1999 (http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html) обучите модель машинного обучения находить сетевые атаки и определять их тип. Точность работы модели необходимо измерять на тестовом наборе данных KDD Cup 1999.
2. Создайте и обучите модель модель машинного обучения для определения злонамеренных сайтов. Для обучения используйте набор данных Malicious and Benign Websites – https://www.kaggle.com/xwolf12/malicious-and-benign-websites

Фонд оценочных материалов (ФОМ) для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине оформляется отдельным документом.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

ДИСЦИПЛИНЫ

6.1. Книгообеспеченность

Наименование литературы: автор, название, вид издания, издательство	Год издания	КНИГООБЕСПЕЧЕННОСТЬ
		Наличие в электронном каталоге ЭБС
Основная литература		
1. Баррат, Д. Последнее изобретение человечества : искусственный интеллект и конец эры Homo sapiens : [пер. с англ.] / Д. Баррат. - 2-е изд. - М. : Альпина нон-фикшн, 2018. - 303 с.	2018	https://www.studentlibrary.ru/book/ISBN9785425702043.html
2. Барский, А. Б. Введение в нейронные сети / Барский А. Б. - Москва : Национальный Открытый Университет "ИНТУИТ", 2016. - Текст : электронный. Режим доступа : по подписке.	2016	https://www.studentlibrary.ru/book/intuit_060.html
3. Хейдт, М. Изучаем pandas / Хейдт М. , пер. с анг. А. В. Груздева. - Москва : ДМК Пресс, 2018. - 438 с. - ISBN 978-5-97060-625-4. - Текст : электронный. Режим доступа : по подписке.	2018	https://www.studentlibrary.ru/book/ISBN9785970606254.html
Дополнительная литература		
1. Флах, П. Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных / Флах П. - Москва : ДМК Пресс, 2015. - 400 с. - ISBN 978-5-97060-273-7. - Текст : электронный. Режим доступа : по подписке.	2015	https://www.studentlibrary.ru/book/ISBN9785970602737.html
2. Рашка, С. Python и машинное обучение : крайне необходимое пособие по новейшей предсказательной аналитике, обязательное для более глубокого понимания методологии машинного обучения / Рашка С. - Москва : ДМК Пресс, 2017. - 418 с. - ISBN 978-5-97060-409-0. - Текст : электронный. Режим доступа : по подписке.	2017	https://www.studentlibrary.ru/book/ISBN9785970604090.html

6.2. Периодические издания

1. Вестник компьютерных и информационных технологий ISSN 1810-7206.

2. Цифровая библиотека научно-технических изданий Института инженеров по электротехнике и радиоэлектронике (Institute of Electrical and Electronic Engineers (IEEE)) на английском языке – http://www.ieee.org/ieeexplore

6.3. Интернет-ресурсы

1. Academic Search Ultimate EBSCO publishing – http://search.ebscohost.com
2. eBook Collections Springer Nature – https://link.springer.com/
3. Гугл Академия – https://scholar.google.ru/
4. Электронно-библиотечная система «Лань» – https://e.lanbook.com/
5. Университетская библиотека ONLINE – https://biblioclub.ru/
6. Электронно-библиотечная система "Библиокомплектатор" (IPRbooks) http://www.bibliocomplectator.ru/available
7. Электронные информационные ресурсы Российской государственной библиотеки https://www.rsl.ru/
8. Научная электронная библиотека «КиберЛенинка» https://cyberleninka.ru/
9. Портал российского образования www.edu.ru

10. Портал российских электронных библиотек www.elbib.ru
11. Научная электронная библиотека www.eLibrary.ru
12. Научная библиотека ВлГУ library.vlsu.ru
13. Электронная библиотечная система ВлГУ https://vlsu.bibliotech.ru/
14. М.В. Ронкин. Курс Time Series Analysis. URL: https://github.com/MVRonkin/Time-Series-Analysis-Lectures-and-Workshops
15. Примеры использования библиотеки SKTimes. URL: https://github.com/sktime/sktime-tutorial-pydata-amsterdam-2020
16. Практический Анализ временных рядов. URL: https://github.com/nmmarcelnv/PracticalTimeSeries
17. Список открытых ресурсов по анализу временных рядов с использованием методов глубокого обучения нейронных сетей. URL: https://github.com/Alro10/deep-learning-time-series
18. Список открытых ресурсов по анализу временных рядов. URL: https://github.com/bifeng/Awesome-time-series
19. Список библиотек анализа временных рядов для языка программирования Python. URL: https://github.com/MaxBenChrist/awesome_time_series_in_python
20. Ресурс, посвященный методам и наборам данных для классификации временных рядов. URL: http://timeseriesclassification.com/index.php
21. Репозиторий, связанный с книгой Practical Time Series Analysis. URL: https://github.com/PracticalTimeSeriesAnalysis/BookRepo
22. Архив наборов данных для анализа временных рядов. URL: https://www.cs.ucr.edu/~eamonn/time_series_data_2018/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для реализации данной дисциплины имеются специальные помещения для проведения занятий: занятий лекционного типа и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы. Практические занятия проводятся в компьютерном классе, оборудованном мультимедийным проектором с экраном и обеспеченным доступом в Интернет.

Перечень используемого лицензионного программного обеспечения:

- Операционная система Microsoft Windows 10
- Офисный пакет Microsoft Office 2016
- Бесплатное программное обеспечение (Python – https://www.python.org/, PyTorch - https://pytorch.org/, TensorFlow, Keras - https://www.tensorflow.org/, Sktime - https://www.sktime.org/en/v0.4.2/, Pandas - https://pandas.pydata.org/, Anaconda solution - https://www.anaconda.com/, Веб - среда разработки для языка программирования Python: google colab - https://colab.research.google.com/)

Рабочую программу составил Куликов К.В. зав. каф. ВТиСУ
(ФИО, должность, подпись)

Рецензент
(представитель работодателя) _____ Генеральный директор ООО "Диаграмма" Протягов И.В.

Программа рассмотрена и одобрена на заседании кафедры ВТ и СУ
Протокол № 1 от 29 августа 2022 года
Заведующий кафедрой Куликов К.В. _____

Рабочая программа рассмотрена и одобрена
на заседании учебно-методической комиссии направления 09.04.01 информатика и вычислительная техника
Протокол № 1 от 29 августа 2022 года
Председатель комиссии Куликов К.В. зав. каф. ВТиСУ_____

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на 20____ / 20____ учебный года
Протокол заседания кафедры № ______ от _________ года
Заведующий кафедрой____

Рабочая программа одобрена на 20____ / 20____ учебный года
Протокол заседания кафедры № ______ от _________ года
Заведующий кафедрой____

Рабочая программа одобрена на 20____ / 20____ учебный года
Протокол заседания кафедры № ______ от _________ года
Заведующий кафедрой____

Рабочая программа одобрена на 20____ / 20____ учебный года
Протокол заседания кафедры № ______ от _________ года
Заведующий кафедрой____

Рабочая программа одобрена на 20____ / 20____ учебный года
Протокол заседания кафедры № ______ от _________ года
Заведующий кафедрой____

Рабочая программа одобрена на 20____ / 20____ учебный года
Протокол заседания кафедры № ______ от _________ года
Заведующий кафедрой____

Рабочая программа одобрена на 20____ / 20____ учебный года
Протокол заседания кафедры № ______ от _________ года
Заведующий кафедрой____

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

в рабочую программу дисциплины

Искусственный интеллект для информационной безопасности

образовательной программы направления подготовки *09.04.01«Информатика и вычислительная техника»*, направленность: *Инженерия искусственного интеллекта (магистратура*)

Номер изменения	Внесены изменения в части/разделы рабочей программы	Исполнитель ФИО	Основание (номер и дата протокола заседания кафедры)

Заведующий кафедрой _____/ _____