Белорусский государственный университет

УТВЕРЖДАЮ
Проректор по учебной работе и образовательным инновациям
_____ О.Н. Здрок
«02» июля 2021 г.

Регистрационный № УД – 10428/уч.

МЕТОДЫ МАШИННОГО ОБУЧЕНИЯ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебная программа учреждения высшего образования по учебной дисциплине для специальности:

1-98 01 01 Компьютерная безопасность (по направлениям)
Направление специальности
1-98 01 01-01 Компьютерная безопасность (математические методы и программные системы)

2021 г.

Учебная программа составлена на основе ОСВО 1-98 01 01-2013 и учебных планов № Р 98-138/уч., № Р 98и-141/уч. от 30.05.2013.

СОСТАВИТЕЛИ:

Курбацкий А.Н., заведующий кафедрой технологий программирования факультета прикладной математики и информатики Белорусского государственного университета, доктор технических наук, профессор;

Ветров Ю.В., ассистент кафедры технологий программирования факультета прикладной математики и информатики Белорусского государственного университета.

РЕЦЕНЗЕНТ:

Пацей Н.В., заведующий кафедрой программной инженерии Белорусского государственного технологического университета, к.т.н., доцент.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой технологий программирования Белорусского государственного университета
(протокол № 16 от 28.05.2021);

Советом факультета прикладной математики и информатики БГУ
(протокол № 11 от 22.06.2021).

Заведующий кафедрой
технологий программирования _____ А.Н. Курбацкий

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели и задачи учебной дисциплины

Цель учебной дисциплины – ознакомление студентов с современными подходами исследования информационной безопасности программных систем на основе методов машинного обучения, формирование теоретических знаний в области распознавания изображений и практических навыков проектирования и разработки моделей машинного обучения.

Задачи учебной дисциплины:

1. Изучение подходов и методов машинного обучения для безопасности программного обеспечения (ПО) и поиска уязвимостей.

2. Формирование практических умений и навыков применения методов машинного обучения для задач распознавания образов и идентификации.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием.

Учебная дисциплина относится **к циклу** дисциплин специализации компонента учреждения высшего образования. В современном информационном обществе существует востребованность в специалистах по архитектуре нейронных сетей для задач распознавания и идентификации, сверточным нейронным сетям, в том числе для задач распознавания изображений.

Программа составлена с учетом **межпредметных связей** с учебными дисциплинами. Основой для изучения учебной дисциплины являются учебные дисциплины I ступени высшего образования «Программирование», «Операционные системы», «Архитектура компьютеров», «Компьютерные сети», «Криптографические методы».

Требования к компетенциям

Освоение учебной дисциплины «Методы машинного обучения в информационной безопасности» должно обеспечить формирование следующих академических, социально-личностных и профессиональных компетенций:

академические компетенции:

АК-1. Уметь применять базовые научно-теоретические знания для решения теоретических и практических задач.

АК-2. Владеть системным и сравнительным анализом.

ЛК-3. Владеть исследовательскими навыками.

АК-4. Уметь работать самостоятельно.

АК-5. Быть способным вырабатывать новые идеи.

АК-9. Уметь учиться, повышать свою квалификацию в течение всей жизни.

социально-личностные компетенции:

СЛК-3. Обладать способностью к межличностным коммуникациям.

СЛК-6. Уметь работать в команде.

профессиональные компетенции:

ПК-1. Работать с научной, нормативно-справочной и специальной литературой с целью получения последних сведений о новых методах защиты информации, о стойкости существующих систем защиты информации.

ПК-2. Формулировать задачи, возникающие при организации защиты информации.

ПК-3. Разрабатывать модели явлений, процессов или систем при организации защиты информации.

ПК-4. Выбирать необходимые методы исследования, модифицировать существующие, разрабатывать новые методы и применять их для решения поставленных задач при организации защиты информации.

ПК-5. Выполнять оценку эффективности методов защиты информации.

ПК-12. Пользоваться глобальными информационными ресурсами.

ПК-13. Владеть современными средствами телекоммуникаций.

ПК-16 Разрабатывать техническое задание на разработку средств и систем защиты информации.

ПК-18. Разрабатывать программные, аппаратно-программные и технические средства и системы защиты информации; разрабатывать необходимую документацию.

ПК-19. Выполнять оценку безопасности реализации средств и систем защиты информации.

В результате освоения учебной дисциплины студент должен:

знать:

- терминологию и понятия машинного обучения;
- архитектуру нейронных сетей для распознавания изображений и идентификации;
- концепции обучения нейронных сетей для задач информационной безопасности.

уметь:

- оценивать эффективность применения методов машинного обучения для задач информационной безопасности;
- обеспечивать критерии оценки применения нейронных сетей для задач информационной безопасности.

владеть:

- навыками решения задач распознавания изображений и идентификации;
- навыками использования методов машинного обучения в информационной безопасности.

Структура учебной дисциплины

Дисциплина изучается в седьмом семестре. Всего на изучение учебной дисциплины «Методы машинного обучения в информационной безопасности» отведено:

– для очной формы получения высшего образования – 159 часов, в том числе 68 аудиторных часов, из них: лекции – 34 часов, лабораторные занятия – 30 часов (в том числе — 12 часов дистанционного обучения с применением ИКТ), управляемая самостоятельная работа – 4 часа дистанционного обучения с применением ИКТ.

Трудоемкость учебной дисциплины составляет 2 зачетные единицы.

Форма текущей аттестации –экзамен.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Раздел 1. Основы машинного обучения в информационной безопасности

Тема 1.1. Введение в машинное обучение

Введение в дисциплину и терминология. Задачи машинного обучения для информационной безопасности. Примеры задач. Виды данных.

Тема 1.2. Основы нейронных сетей для задач информационной безопасности

Введение в нейронные сети для задач информационной безопасности. Многослойные сети прямого распространения. Концепция обучения. Градиентный спуск. Метод обратного распространения ошибки.

Раздел 2. Архитектура нейронных сетей для задач распознавания и идентификации

Тема 2.1. Сверточные нейронные сети

Архитектура сверточных нейронных сетей. Сверточные сети для решения классической задачи распознавания символов. Дополнительные техники обучения. Оптимизаторы и их виды. Скорость обучения. Другие параметры оптимизаторов. Регуляризация и дропауты как способы борьбы с переобучением нейронных сетей. Практические примеры с применением набора инструментов для проектирования и тренировки сетей различного типа (Computational Network Toolkit — CNTK) на примере Microsoft Cognitive Toolkit, библиотек Keras, TensorFlow и языков программирования C# b Python.

Тема 2.2. Сиамские нейронные сети в задачах идентификации

Архитектура сиамских нейронных сетей. Сиамский нейронные сети для задач идентификации и распознавания лиц. Построение и обучение модели для задачи распознавания лиц. Практические примеры с применением библиотек Keras, TensorFlow и языка программирования Python.

Раздел 3. Нейронные сети для задач распознавания изображений

Тема 3.1. Основы нейронных сетей для задач распознавания изображений

Архитектура нейронных сетей для задач распознавания изображений. Примеры задач распознавания объектов. Неройнные сети типа R-CNN и Fast R-CNN для решения распознавания объектов. Построение и обучение модели для задачи распознавания объектов в области информационной безопасности. Практические примеры с применением библиотек Keras, TensorFlow и языка программирования Python.

Тема 3.2. Семантическая сегментация изображений

Понятие семантической сегментации. Encoder и Decoder. Архитектура нейросети для задачи семантической сегментации. Маска изображения на примере R-CNN. Нейронная сеть FCN в задачах сегментации.

Тема 3.3. Дополнительные техники обучения и генетические алгоритмы

Применение дополнительных техник обучения нейронных сетей. Алгоритм Левенберга-Марквардта для оптимизации параметров нелинейных регрессионных моделей. Генетические и эволюционные алгоритмы. Генетические алгоритмы для решения задач оптимизации.

Преимущества и особенности генетических алгоритмов.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Дневная форма получения образования с применением дистанционных образовательных технологий

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	2	3	4	5	6	7	8	9
1	**Основы машинного обучения в информационной безопасности**	**6**			**4**			
1.1	Введение в машинное обучение	2			2			собеседование
1.2	Основы нейронных сетей для задач информационной безопасности	4			2			отчет
2	**Архитектура нейронных сетей для задач распознавания и идентификации**	**18**			**6** **4 (ДО)**		**2 (ДО)**	
2.1	Сверточные нейронные сети	10			4 2 (ДО)			проект
2.2	Сиамские нейронные сети в задачах идентификации	8			2 2 (ДО)		2 (ДО)	отчет
3.	**Нейронные сети для задач распознавания изображений**	**10**			**8** **8 (ДО)**		**2 (ДО)**	
3.1	Основы нейронных сетей для задач распознавания изображений	6			2 4 (ДО)			коллоквиум
3.2	Семантическая сегментация изображений	4			4 4 (ДО)			реферат
3.3	Дополнительные техники обучения и генетические алгоритмы				2		2 (ДО)	отчет
	Всего	**34**			**30**		**4**	

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень основной литературы

1. Бринк Х. Машинное обучение. / Х. Бринк, Дж. Ричардс, Ф. Феверолф. — СПб.: Питер, 2017. — 336 с.: ил. — (Серия «Библиотека программиста»).

2. Кухарев Г. А. Методы обработки и распознавания изображений лиц в задачах биометрии / Г. А. Кухарев, Е. И. Каменская, Ю. Н. Матвеев, Н. Л. Щеголева; под ред. М. В. Хитрова. — СПб.: Политехника, 2013. — 388 с.: ил.

3. Паклин Н.Б. Бизнес-аналитика: от данных к знаниям: учеб. пособие / Н. Паклин, В. Орешков. — 2-е изд., доп. и перераб. — СПб.: Питер, 2010. — 701 с.

4. Николенко, С. Глубокое обучение. Погружение в мир нейронных сетей / С. Николенко, А. Кадурин, Е. Архангельская. — СПб.: Питер, 2020. — 476 с.

5. Мэтиз, Эрик. Изучаем Python = Python Crash Course : программирование игр, визуализация данных, веб-приложения / Э. Мэтиз ; [перевел с англ. Е. Матвеев]. — 3-е изд. — СПб.: Питер, 2020. — 511 с.

6. Плас, Джейк Вандер. Python для сложных задач: наука о данных и машинное обучение / Дж. Вандер Плас; [пер. с англ. И. Пальти]. — СПб.: Питер, 2018. — 573 с.

Перечень дополнительной литературы

1. Вьюгин В.В. Математические основы теории машинного обучения и прогнозирования. — М.: 2013. — 387 с.

2. Николенко С., Тулупьев А. Самообучающиеся системы. — М.: МЦНМО, 2009. — 288 с.

3. Жерон О. Прикладное машинное обучение с помощью Scikit-Learn и TensorFlow: концепции, инструменты и техники для создания интеллектуальных систем / пер. с англ. — М.: Диалектика, 2018. — 688 с.

4. Силен, Дэви. Основы Data Science и Big Data. Python и наука о данных / Дэви Силен, Арно Мейсман, Мохамед Али ; [пер. с англ. Е. Матвеева]. — СПб.: Питер, 2017. — 334 с.

5. Christopher M. Bishop. Pattern Recognition and Machine Learning. — Springer, Information Science and Statistics series, 2006. — 738 pp.

Перечень рекомендуемых средств диагностики и методика формирования итоговой оценки

Для диагностики компетенций в рамках учебной дисциплины рекомендуется использовать следующие формы:

1) Устная форма: собеседование, коллоквиум.

2) Письменная форма: отчет по лабораторным работам с устной защитой и оцениванием на основе модульно-рейтинговой системы.

Формой текущей аттестации по дисциплине «Методы машинного обучения в информационной безопасности» учебным планом предусмотрен экзамен.

При формировании итоговой оценки используется рейтинговая оценка знаний студента, дающая возможность проследить и оценить динамику процесса достижения целей обучения. Рейтинговая оценка предусматривает использование весовых коэффициентов для текущего контроля знаний и текущей аттестации студентов по дисциплине.

Примерные весовые коэффициенты, определяющие вклад текущего контроля знаний и текущей аттестации в рейтинговую оценку.

Формирование оценки за текущую успеваемость:

- отчет по лабораторным работам – 50 %;
- коллоквиум – 10%;
- проект – 20%;
- реферат – 10%;
- собеседование – 10 %.

Рейтинговая оценка по дисциплине рассчитывается на основе оценки текущей успеваемости и экзаменационной оценки с учетом их весовых коэффициентов. Весовой коэффициент оценки по текущей успеваемости составляет 40 %, экзаменационной оценки – 60 %.

Примерный перечень заданий для управляемой самостоятельной работы студентов

Управляемая самостоятельная работа (консультационно-методическая поддержка и контроль) осуществляться преимущественно в дистанционной форме и обеспечивается средствами образовательного портала БГУ (LMS Moodle).

В отдельных случаях управляемая самостоятельная работа проводится в форме аудиторных занятий, согласно утвержденному графику.

Объем часов на составление и размещение заданий, консультации и контроль, осуществляемые с использованием технологий дистанционного обучения, планируется в пределах учебных часов, отведенных на УСР.

Тема 2.2. Сиамские нейронные сети в задачах идентификации (2 ч/ДО)

Построение и обучение модели для задачи распознавания лиц.

Обсуждение и анализ практических примеров обучение моделей нейронных сетей для задач распознавания лиц с применением библиотек Keras, TensorFlow и языка программирования Python.

Анализ данных на платформе https://kaggle.com или решение других исследовательских задач. Обеспечение на образовательном портале – инструкция по выполнению проектов.

Форма контроля – отчет по лабораторным работам.

Тема 3.3. Дополнительные техники обучения и генетические алгоритмы (2 ч/ДО)

Генетические алгоритмы для решения задач оптимизации.

Анализ и применение генетических алгоритмов для задач оптимизации и идентификации объектов.

Форма контроля – отчет по лабораторным работам.

Примерная тематика лабораторных занятий

Лабораторная работа № 1. Поиск и распознавание символов на номерном знаке автомобиля

Лабораторная работа № 2. Распознавание лиц с помощью сиамских нейронных сетей

Лабораторная работа № 3. Построение модели Faster R-CNN для задачи object detection

Рекомендуемая тематика коллоквиума:

1. Коллоквиум «Методы машинного обучения для распознавания и идентификации объектов в задачах информационной безопасности».

Текущий контроль знаний проводится в соответствии с учебно-методической картой дисциплины.

Описание инновационных подходов и методов к преподаванию учебной дисциплины

При организации образовательного процесса используются ***метод анализа конкретных ситуаций (кейс-метод) и метод проектного обучения***.

Кейс-метод предполагает:

- приобретение студентом знаний и умений для решения практических задач в области обеспечения информационной безопасности;
- анализ ситуации, используя профессиональные знания, собственный опыт, дополнительную литературу и иные источники по теме дисциплины.

Метод проектного обучения обеспечивает**:**

- способ организации учебной деятельности студентов, развивающий актуальные для учебной и профессиональной деятельности навыки

планирования, самоорганизации, сотрудничества и предполагающий создание собственного продукта;

- приобретение навыков для решения исследовательских, творческих, социальных, предпринимательских и коммуникационных задач.

Методические рекомендации по организации самостоятельной работы обучающихся

Для организации самостоятельной работы студентов по учебной дисциплине следует использовать современные информационные ресурсы: разместить на образовательном портале комплекс учебных и учебно-методических материалов (учебно-программные материалы, учебное издание для теоретического изучения дисциплины, методические указания к лабораторным занятиям, материалы текущего контроля и текущей аттестации, позволяющие определить соответствие учебной деятельности обучающихся требованиям образовательных стандартов высшего образования и учебно-программной документации, в т.ч. вопросы для подготовки к зачету, задания, тесты, вопросы для самоконтроля, тематика рефератов и др., список рекомендуемой литературы, информационных ресурсов и др.).

Темы реферативных работ

1. Обзор методов машинного обучения для задач информационной безопасности (не рассматриваемых в рамках учебной дисциплины)
2. Обзор методов машинного обучения для задач биометрии
3. Компьютерная безопасность и машинное обучение

Примерный перечень вопросов к экзамену

1. Задачи машинного обучения для информационной безопасности.
2. Нейронные сети и задачи информационной безопасности.
3. Многослойные сети прямого распространения.
4. Концепция обучения.
5. Градиентный спуск.
6. Метод обратного распространения ошибки.
7. Архитектура сверточных нейронных сетей.
8. Сверточные сети для решения классической задачи распознавания символов.
9. Оптимизаторы и их виды.
10. Способы борьбы с переобучением нейронных сетей.
11. Архитектура сиамских нейронных сетей.
12. Сиамские нейронные сети для задач идентификации и распознавания лиц.
13. Архитектура нейронных сетей для задач распознавания изображений.

14. Неройнные сети типа R-CNN и Fast R-CNN для решения распознавания объектов.

15. Построение и обучение модели для задачи распознавания объектов в области информационной безопасности.

16. Семантическая сегментация изображений.

17. Нейронные сети для задач семантической сегментации.

18. Дополнительные техники обучения нейронных сетей.

19. Алгоритм Левенберга-Марквардта.

20. Генетические и эволюционные алгоритмы.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ УВО

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Безопасность операционных систем	Технологий программирования	Нет	Оставить содержание учебной дисциплины без изменения, протокол № 16 от 28.05.2021

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ ПО ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ

на _____/_____ учебный год

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры
_____ (протокол № ____ от _____ 20__ г.)

Заведующий кафедрой
_____ _____ _____

УТВЕРЖДАЮ
Декан факультета
_____ _____ _____