УДК 614

АФАНАСЬЕВ АЛЕКСАНДР ДИОМИДОВИЧ,
АФАНАСЬЕВА ЖАННА СЕРГЕЕВНА,
МИЛЬКО ДМИТРИЙ СЕРГЕЕВИЧ

МЕТОДИЧЕСКИЕ ОСОБЕННОСТИ ПРАКТИКУМА ПО ИСКУССТВЕННОМУ ИНТЕЛЛЕКТУ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

АННОТАЦИЯ

В статье сообщается об основных принципах и методических особенностях построения лабораторного практикума по изучению искусственного интеллекта и машинного обучения для студентов уровня бакалавриата. Обсуждается связь лабораторных работ практикума с компетенциями ФГОС, утверждённого приказом Министерства образования и науки Российской Федерации от 1 декабря 2016 г. по направлению подготовки 10.03.01 Информационная безопасность.

Ключевые слова: методика преподавания; лабораторный практикум; информационная безопасность; искусственный интеллект; машинное обучение.

AFANASIEV A.D.,
AFANASIEVA J.S.,
MILKO D.S.

METHODICAL SPECIFICS OF ARTIFICAL INTELLECT PRACTICUM IN INFORMATION SECURITY SPHERE

ABSTRACT

The article deals with the main principles and methodological peculiarities of the laboratory practical work on the study of artificial intellect and machine learning for undergraduate students. The connection of laboratory works with the workshop with the competencies of Federal State Education Standards (approved by the Ministry of Education and Science of the Russian Federation in December 1st, 2016) in the 10.03.01 Information security major, is discussed.

Keywords: teaching methodology; laboratory practicum; information security; artificial intellect; machine learning.

Крупнейшие мировые компании в области информационной безопасности (ИБ) в своих аналитических отчетах прогнозируют новые тенденции, связанные со значительным развитием технологий искусственного интеллекта (AI) и машинного обучения (ML) и их применений для практических задач. В прогнозных докладах от Digital Security «Аналитика по кибербезопасности за 2016-2017» [1], в аналитическом отчете от «Positive Technologies» [2], годовом отчете «Cyber Risk Report: 2016 Cybercrime Trends Year-in-Review» [3] и в статье издания CIO [4], говорится о том, что в решениях безопасности станет больше функциональности, связанной с AI и ML. Популяризация идей, связанных с машинным обучением, рост количества фреймворков, помогающих в этом, влечет за собой создание новых продуктов ИБ, которые будут использовать данный подход.

В статье «Машинное обучение: надежда в борьбе с кибератаками» авторы отмечают, что «машинное обучение — крупнейшая тенденция в области безопасности в текущем году». «Сегодня любой директор по информационной безопасности знает, что средства поведенческого анализа дают наилучшие шансы остановить атаку, способную обойти статичные защитные системы» [5]. Это мнение поддерживает Димитриос Павлакис, отраслевой аналитик компании ABI Research, он говорит: «Мы находимся в разгаре революции искусственного интеллекта в сфере безопасности. Благодаря этому, машинное обучение вскоре станет новой нормой, наравне с информационной безопасностью, управлением событиями или SIEM, и, в конечном итоге, в течение ближайших пяти лет вытеснит большую часть традиционных антивирусов, эвристики и систем на основе сигнатур» [6].

Таким образом, тенденции, связанные с развитием данных технологий определяют необходимость изучения искусственного интеллекта и машинного обучения студентами, обучающимися по ИБ.

Проблема, связанная с обучением AI и ML, в том, что в литературных источниках нет системно изложенного материала для преподавания лабораторных работ, чтобы он был «заточен» под задачи по информационной безопасности и связан с действующим ФГОС и современными профессиональными стандартами.

Нами разработан комплекс лабораторных работ для студентов-бакалавров. Освоение комплекса базируется на исследовательских заданиях, с опорой на творческий потенциал студента и обеспечивает развитие ряда базовых компетенций в области ИБ.

Комплекс состоит из семи лабораторных работ по изучению Искусственного интеллекта:

1. Метод отжига;
2. Обучение персептрона;
3. Нейронная сеть Хопфилда;
4. Классификация сетью Кохонена;
5. Самоорганизующиеся карты Кохонена;
6. Генетические алгоритмы;
7. Обучение с подкреплением.

В лабораторном практикуме реализуются ряд научных и дидактических принципов, которые созвучны рекомендациям, изложенным в работе [7].

Создание высокоинтеллектуальных машин удел талантливых людей. Основа развития таланта – заинтересованность студента. А заинтересованность студента во многом формируется заботливым участием преподавателя, его искусством направлять творческий потенциал студента, создавать позитивную рабочую атмосферу для его успешного развития.

Мощный стимул для формирования заинтересованности – это достижение результатов. Получая последовательные результаты сначала для простых учебных задач, затем для более сложных, а в перспективе – для научных проблем, студент вовлекается в творческий процесс. Принцип движения от простого к сложному лежит в основе разработанного нами лабораторного комплекса. Следуя этому принципу, были сформулированы практические задания в лабораторных работах.

Среди изобилия методов изучения AI и ML на практике мы использовали два подхода. Первый основан на знании студентом программирования и позволяет в деталях проработать алгоритм какого-либо метода, используя возможности изменять код программы. Преимущество такого подхода в том, что можно варьировать основные параметры, применяемые в алгоритме, модифицировать сам алгоритм и проводить множество экспериментов, изучая свойства метода. К сожалению, требование знания языка программирования ограничивает аудиторию учащихся.

Другой подход основан на использовании специализированных программ по AI и ML. Он хорош тем, что не требуется знания языков программирования и тем, что результат даже для сложных систем достигается сравнительно быстро.

Мы использовали преимущества обоих подходов, опираясь на то, что студенты технического направления изучают программирование. Однако, старались подбирать задания, не требующие глубокого знания языков. Преимущество такого сочетания подходов в том, что оно позволяет, с одной стороны, проводить со студентами глубокое изучение сути метода, а затем, используя стандартные программы, исследовать его возможности в практических приложениях.

Основная сложность заключается в том, что в большинстве книг материалы по AI и ML излагаются в теоретическом виде, в виде схем методов,

которые не всегда понятны студентам. Как правило, для понимания студентам требуется практическая реализация методов. Для эффективного обучения важно создать условия, когда обучающийся сам сможет запрограммировать простейшие примеры методов AI и ML и увидеть их работу.

Среди множества литературы по AI и ML выгодно выделяются лекции профессора Р. В. Шамина [8]. Его лекции построены по принципу – любой метод или алгоритм реализуется в виде работающей программы, которую можно скачать и опробовать. Видеозаписи его лекций выложены в интернете [9]. Практически все базовые алгоритмы AI и ML обсуждаются в лекциях Р.В. Шамина. Лекции снабжены работающими компьютерными программами для проведения самостоятельных исследований. Основными языками программирования, которые использует Р. В. Шамин, являются Python и C#. Он считает, что для реализации программ искусственного интеллекта наиболее подходящим является Python, а для создания красивого графического интерфейса лучше использовать C#.

Помимо названных языков в лабораторном практикуме используются специализированные пакеты, предназначенные для создания и работы с нейронными сетями. Например, STATISTICA Automated Neural Networks (SANN). Такие пакеты программ имеют ряд полезных возможностей и, кроме того, ими могут пользоваться студенты, не знающие в должной мере языки программирования.

Задания в лабораторном практикуме сформулированы таким образом, чтобы побудить студента к исследовательской деятельности в процессе выполнения каждого пункта лабораторной работы. Задания, в которых студенту предлагается «…изучить влияние параметра на эффективность…», «…исследовать, как зависят результаты от…», «…выяснить какие значения параметров являются оптимальными…» вовлекают студента в исследовательскую деятельность. Таким образом, с методической точки зрения при соответствующей квалификации преподавателя создается творческая атмосфера, способствующая эффективному продвижению в изучении курса.

По окончании лабораторного практикума студенту предлагается на выбор исследовательский проект с использованием одного из изученных методов AI и ML. Проект выполняется в течение года как курсовой и защищается в конце курса. При этом приветствуется привлечение дополнительных ресурсов, в частности, людских ресурсов (не обязательно из университета). Возможно объединение в команды.

Другим стимулом для студентов является участие их проектов в конкурсе. Победители конкурса получают ценные финансовые и моральные призы.

С целью углубления профессиональной направленности лабораторного практикума было изучено соответствие компетенций и профстандартов в приложении к машинному обучению.

Из ФГОС по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата) можно выделить 3 основных компетенции (ОПК-4, ПК-2, ПК-12), которые формируются в ходе выполнения лабораторных работ студенты. Формулировки этих компетенций приведены в Таблице 1.

Для установления соответствия между названными компетенциями и профессиональными стандартами был проведен анализ 7 профессиональных стандартов в области информационной безопасности: «Специалист по защите информации в автоматизированных системах», «Руководитель проектов в области информационных технологий», «Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности», «Специалист по безопасности компьютерных систем и сетей», «Менеджер по информационным технологиям», «Специалист по защите информации в телекоммуникационных системах и сетях», «Специалист по технической защите информации».

Результаты анализа представлены в Таблице 1. Отобранные компетенции (ОПК-4, ПК-2, ПК-12) представлены в первой строке таблицы. В столбце представлены трудовые функции, трудовые действия и необходимые умения, которые, по нашему мнению, соответствуют отобранным компетенциям.

Из 7 профессиональных стандартов, с учетом уровня бакалавриата (уровень квалификации 6), соответствие установлено лишь для 2 трудовых функций профессионального стандарта «Специалист по защите информации в автоматизированных системах». В пересечениях между отобранными компетенциями и трудовыми

Таблица 1

Соответствие компетенций профессиональному стандарту по направлению ИБ (уровень бакалавриата).

Наименование компетенции		*ОПК-4 Способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации*	*ПК-2 Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы*	*ПК-12 Способность принимать участие в проведении экспериментальных исследований системы защиты информации*
Специалист по защите информации в автоматизированных системах				
Диагностика систем защиты информации автоматизированных систем B/01.6				
Трудовые действия	Идентификация инцидентов в процессе эксплуатации автоматизированной системы	Обосновано необходимостью поиска дополнительных сведений об особенностях инцидентов безопасности	Обосновано необходимостью применения перечисленных средств для идентификации инцидентов	Идентификация инцидентов требует проведения экспериментальных исследований
	Оценка защищенности автоматизированных систем с помощью типовых программных средств	-	Обосновано необходимостью применения перечисленных средств для оценки защищенности	Оценка защищенности требует проведения экспериментальных исследований
Необходимые умения	Применять технические средства контроля эффективности	-	Обосновано необходимостью применения инструментальных средств контроля эффективности	Контроль эффективности осуществляется, в том числе с применением экспериментальных исследований
Аудит защищенности информации в автоматизированных системах B/06.6				
Необходимые умения	Применять инструментальные средства контроля защищенности в автоматизированных системах	-	Обосновано необходимостью применения инструментальных средств контроля защищенности	Контроль защищенности осуществляется, в том числе с применением экспериментальных исследований

действиями, необходимыми умениями нами сформулировано краткое обоснование соответствия.

Таким образом, разработанный лабораторный практикум формирует 3 компетенции, которые представлены в профессиональном стандарте, т.е. одобрены работодателями.

Список литературы

1. Digital Security: прогноз тенденций и угроз ИБ-2017. [Электронный ресурс]. – Режим доступа: https://dsec.ru/news/press/digital_security_forecast_of_the_trends_and_threats_to_information_security_2017/ (дата обращения 26.11.2017).

2. Аналитика. Positive Technologies. [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/ (дата обращения 26.11.2017).

3. M-Trends 2017 Cyber Security Trends. [Электронный ресурс]. – Режим доступа: https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html (дата обращения 26.11.2017).

4. Информационная безопасность в 2017 году: тенденции. [Электронный ресурс]. – Режим доступа: https://www.osp.ru/cio/2017/1/13051454/ (дата обращения 26.11.2017).

5. Машинное обучение надежда в борьбе с кибератаками. [Электронный ресурс]. – Режим доступа: https://www.cio.ru/articles/1043 (дата обращения 26.11.2017).

6. Машинное обучение в области кибербезопасности станет причиной возникновения большого объема данных, информации и роста расходов на аналитику. [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/blog/personal/tsarev/339164.php . (дата обращения 26.11.2017).

7. *Чернобровкина И. И.* Методологическое обеспечение организации лабораторного практикума по дисциплинам искусственного интеллекта // Открытое и дистанционное образование. – 2015. – № 58. – Т. 2. – с. 35-40.

8. *Курс Р. В.* Шамина «Машинное обучение и искусственный интеллект в математике и приложениях». [Электронный ресурс]. – Режим доступа: http://www.mathnet.ru/conf1243 (дата обращения 29.11.2017 г.).

9. *Шамин Р. В.* Лекции по машинному обучению и искусственному интеллекту в МИАН. [Электронный ресурс]. – Режим доступа: https://www.youtube.com/playlist?list=PLEaWFQiR5rGP2lbmBaybBWmBqvM6XlknL (дата обращения 25.11.2017 г.).

Статья поступила в редакцию 6 ноября 2017 г.