

Разработка программы повышения квалификации «Искусственный интеллект и кибербезопасность: защита данных в цифровую эпоху»

Ю.А. Крыжановская, Н. В. Дорофеев, А.В. Христофорова, Т.А. Николаев, Т.В. Митрофанова,
В.Ю. Герасин, О.И. Аширова

Аннотация — В 2024-2025 учебном году Альфа банк и университет ИТМО инициировали и провели программу "Современный искусственный интеллект в высшей школе", в данной статье представлен итоговый проект, выполненный группой разработчиков, представляющих шесть университетов Воронежа, Казани, Москвы, Муром, Чебоксар. В качестве предварительного этапа был проведен анализ ряда аналогичных существующих решений, что позволило обосновать структуру и содержание представленной программы. Программа разработана для специалистов, стремящихся не только расширить свои знания в области информационной безопасности, но и освоить современные технологии искусственного интеллекта для защиты данных. Программа объединяет три основных направления: изучение основ ИИ и его применения в кибербезопасности, практическая работа по выявлению и предотвращению угроз с помощью ИИ, анализ этических и правовых аспектов применения технологий ИИ. Она не только предоставляет теоретическую базу, но и акцентируется на практическом применении знаний в современных цифровых экосистемах. Ключевой целью является подготовка специалистов, которые смогут эффективно применять ИИ для решения задач мониторинга, анализа и предотвращения атак в условиях современных цифровых вызовов. Формат программы предполагает командную работу, что позволяет участники погрузиться в реальные сценарии угроз и отработать практические навыки. Итогом становится комплексный проект, в котором команды объединяют свои знания, чтобы разработать решения для защиты условной корпоративной системы, учитывая современные технологии ИИ и киберугрозы. Программа подходит как для повышения квалификации, так и для карьерного перехода.

Ключевые слова — кибербезопасность, искусственный интеллект, повышение квалификации, методики обучения.

I. ВВЕДЕНИЕ

Технологии искусственного интеллекта (ИИ) [1] постепенно проникают практически во все области деятельности человека, находя применение в обработке текстов на естественных языках [2] и мультимедийного контента [3], стеганографии [4], для решения задачи классификации в судебной медицине [5], в банковской сфере [6], а также во многих других сферах, включая кибербезопасность [7].

Согласно статистике, 85% кибератак связаны с применением ИИ, что говорит о том, что существующие представления об информационной безопасности устаревают. Новым направлением в информационной безопасности является безопасность самого искусственного интеллекта [8-10]. В работе [11] анализируются ключевые вопросы на стыке ИИ и кибербезопасности. Использование искусственного интеллекта в кибербезопасности в последние годы становится растущей областью исследований и применения. Методы искусственного интеллекта, такие как машинное обучение, глубокое обучение, обработка естественного языка и системы, основанные на знаниях, обладают потенциалом для улучшения различных задач кибербезопасности, включая обнаружение угроз, выявление аномалий, анализ уязвимостей и управление безопасностью [12-21].

Развитие и распространение технологий ИИ привело к необходимости подготовки специалистов в области как кибербезопасности, так и искусственного интеллекта [22-26].

Развитию темы подготовки специалистов в области безопасности и применения технологий искусственного интеллекта посвящена данная работа. В 2024-2025 учебном году Альфа банк и университет ИТМО инициировали и провели программу "Современный искусственный интеллект в высшей школе", в которой на конкурсной основе приняли 150 участников из разных городов России. Программа включала три трека: трек 1 «Введение в возможности искусственного

Статья получена 23 июня 2026.

Ю. А. Крыжановская – Воронежский государственный университет, Воронеж, Россия (e-mail: jak@mail.ru)

Н. В. Дорофеев – Владимирский государственный университет имени А.Г. и Н.Г. Столетовых, Муром, Россия (e-mail: dorofeevny@yandex.ru)

А. В. Христофорова – Чувашский государственный университет им. И.Н. Ульянова, Чебоксары, Россия (e-mail: dlya.nastenki@mail.ru)

Т. А. Николаев – Казанский инновационный университет им. В. Г. Тимирязева, Казань, Россия (e-mail: timur_nikolaev@inbox.ru)

Т. В. Митрофанова – Чувашский государственный университет им. И.Н. Ульянова, Чебоксары, Российская Федерация (e-mail: mitrofanova_tv@mail.ru)

В. Ю. Герасин – МИРЭА – Российский технологический университет, Колледж программирования и кибербезопасности, Москва, Россия (e-mail: gerasin.vladislav@mail.ru)

О. И. Аширова – Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия (e-mail: ashirova-oi@pfur.ru)

интеллекта», трек 2 «Технологии искусственного интеллекта и их применение», трек 3 «Преподавание искусственного интеллекта в университете» (продвинутый уровень). На очной защите было представлено 29 проектов. В данной статье описан проект трека 3, выполненный группой разработчиков, представляющих шесть университетов Воронежа, Казани, Москвы, Муром, Чебоксар, программы повышения квалификации «Искусственный интеллект и кибербезопасность: защита данных в цифровую эпоху».

II. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

A. Анализ существующих решений

Для обоснования актуальности и новизны разработанной программы повышения квалификации «Искусственный интеллект и кибербезопасность: защита данных в цифровую эпоху» в качестве предварительного этапа был проведён анализ ряда реализуемых в Российской Федерации программ дополнительного профессионального образования, ориентированных на формирование компетенций в области информационной безопасности и применения технологий искусственного интеллекта:

- ИИ: применение в ИБ (РосНОУ), <https://rosnou.ru/dpo/cdpo/advanced-training/iskusstvennyy-intellekt-primeneniye-v-informatsionnoy-bezopasnosti/>;
- ИИ для информационной безопасности (Академия информационных систем), https://www.infosystems.ru/courses/avtorskie_kursy/IS118/;
- Информационная безопасность. Обеспечение безопасности компьютерных систем и сетей (Академия Ай Ти), <https://edu.softline.com/api/programm/5096575/>;
- Современные технологии ИИ: внедрения и эффекты (ВШЭ), <https://miem.hse.ru/dpo/announcements/964625383.html>.

Источниками служили официально опубликованные учебные планы и программы, размещённые на сайтах организаций.

Анализ показал, что большинство российских программ повышения квалификации в рассматриваемой предметной области ориентированы преимущественно на одну из двух составляющих – либо на классическую информационную безопасность, либо на прикладные аспекты искусственного интеллекта, без их системной интеграции. Так, программы, реализуемые в коммерческом и корпоративном секторе (например, курсы Академии АйТи или специализированных центров повышения квалификации), в основном фокусируются на вопросах нормативно-правового обеспечения информационной безопасности, архитектуре защищённых сетей, анализе уязвимостей и эксплуатации средств защиты информации. При этом технологии искусственного интеллекта рассматриваются фрагментарно и, как правило, без глубокого анализа рисков, связанных с безопасностью самих ИИ-систем.

Вузовские программы повышения квалификации, ориентированные на применение искусственного интеллекта в информационной безопасности, как правило, имеют ограниченную модульную структуру и сравнительно небольшой объём. Например, отдельные курсы включают модули, посвящённые использованию методов машинного обучения для обнаружения атак или анализа сетевого трафика, однако не охватывают вопросы социальной инженерии, устойчивости ИИ-моделей к целенаправленным атакам (*adversarial attacks*), а также этические и правовые аспекты применения ИИ в системах безопасности. В большинстве случаев такие программы направлены на обновление профессиональных знаний специалистов и не предполагают формирования комплексной междисциплинарной модели компетенций.

В связи с этим в качестве существенного отличия представляемой программы от существующих решений был предложен и реализован её комплексный характер и ориентация на формирование целостного набора компетенций на стыке искусственного интеллекта и кибербезопасности. В отличие от аналогов, программа предполагает охват не только применения ИИ для решения задач обнаружения и предотвращения кибератак, но и вопросы защиты самих ИИ-систем, анализа угроз, связанных с манипуляцией данными и моделями, а также проблемы социальной инженерии и человеческого фактора. Отдельное внимание предложено уделить этическим и правовым аспектам использования технологий искусственного интеллекта, что в большинстве анализируемых программ либо отсутствует, либо рассматривается декларативно.

Дополнительным преимуществом представленной программы предполагается её нормативная и профессиональная обоснованность. Проектирование программы должно учитывать действующие федеральные законы в сфере образования и защиты персональных данных, а также опираться на профессиональные стандарты, связанные с цифровой грамотностью, анализом больших данных и автоматизацией информационно-аналитической деятельности. В ряде существующих программ подобная связь с профессиональными стандартами либо не декларируется, либо носит формальный характер, что затрудняет оценку соответствия формируемых компетенций требованиям рынка труда.

Сравнительный анализ также показал, что большинство аналогичных программ используют преимущественно лекционно-практическую модель обучения без развернутой проектной компоненты. В представленной программе, напротив, ключевым элементом было решено сделать командную проектную деятельность, моделирующую реальные сценарии киберугроз и защиты корпоративных информационных систем с применением технологий искусственного интеллекта. Это может позволить не только закрепить теоретические знания, но и сформировать практические навыки принятия решений в условиях неопределённости и многофакторных рисков.

Полученные результаты анализа подтверждают целесообразность реализации новой программы и её потенциальную востребованность в условиях трансформации цифровых экосистем и роста ИИ-ориентированных киберугроз.

В. Аннотация Программы

Программа предназначена для специалистов с техническим / физико-математическим образованием, которые хотят приобрести новые компетенции в области информационной безопасности и научиться использовать технологии искусственного интеллекта (ИИ) для защиты данных в современных цифровых системах.

Настоящая примерная программа повышения квалификации «Искусственный интеллект и кибербезопасность: защита данных в цифровую эпоху» (далее – программа повышения квалификации, программа) разработана с учетом положений:

- Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» (<http://publication.pravo.gov.ru/document/0001201212300007>);
- Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (<https://72.rkn.gov.ru/p21978/p25026/p25030/>);
- приказа Минобрнауки России от 1 июля 2013 г. № 499 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам» (<https://base.garant.ru/70440506/>);
- профессионального стандарта «Консультант в области развития цифровой грамотности населения (цифровой куратор)», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 31.10.2018 № 682н (<https://base.garant.ru/72108006/>);
- профессионального стандарта «Специалист по большим данным», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 06.07.2020 № 405н (https://www.consultant.ru/document/cons_doc_LAW_359468/);
- профессионального стандарта «Специалист по автоматизации информационно-аналитической деятельности», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 20.07.2022 № 425н (https://www.consultant.ru/document/cons_doc_LAW_425012/).

С. Цели и задачи Программы

Цель программы состоит в подготовке специалистов, способных внедрять и применять решения на базе ИИ для защиты корпоративной инфраструктуры и предотвращения кибератак с учетом требований к соблюдению этических норм.

Задачи программы:

1. Обучение применению ИИ в информационной безопасности.
2. Изучение методов защиты данных и предотвращения утечек при использовании ИИ-технологий.

3. Освещение вопросов этики при разработке и внедрении ИИ в информационные системы.

4. Изучение угроз, связанных с применением ИИ в кибератаках, а также разработка методов противодействия.

5. Подготовка к использованию ИИ для анализа данных, обнаружения угроз и автоматизации управления безопасностью.

С. Компетенции (трудовые функции) в соответствии с Профессиональным стандартом

Программа направлена на формирование у слушателей ключевых компетенций, необходимых для работы на стыке искусственного интеллекта и кибербезопасности. Среди них:

- Анализ и мониторинг угроз с помощью ИИ: слушатели научатся применять технологии машинного обучения для автоматического обнаружения аномалий, анализа сетевого трафика и предсказания кибератак.
- Разработка методов защиты ИИ-систем, включая создание устойчивых моделей, защищенных от атак.
- Выявление угроз информационной безопасности: обучение методам противодействия социальным атакам и манипуляциям с использованием данных.
- Этическая и правовая экспертиза: умение учитывать национальные и международные нормы при разработке и внедрении решений, которые используют ИИ.

Эти компетенции позволят участникам не только адаптироваться к современным вызовам, но и внедрять передовые решения для защиты данных и инфраструктуры.

Д. Планируемые результаты обучения

В рамках программы слушатели приобретут всесторонние знания и навыки, необходимые для работы с технологиями искусственного интеллекта в области кибербезопасности. Они изучат принципы работы ИИ, методы машинного обучения и современные угрозы. Особое внимание уделено практическим подходам к автоматизации процессов информационной безопасности и защите данных в соответствии с правовыми нормами. Слушатели научатся разрабатывать и внедрять решения для анализа сетевого трафика, обнаружения аномалий и предотвращения атак.

Кроме того, программа готовит к применению этических и правовых норм при интеграции ИИ в системы безопасности, что особенно важно в современных реалиях.

Е. Категории слушателей

Программа ориентирована на широкий круг специалистов. В первую очередь она будет полезна IT-специалистам, желающим внедрять и управлять решениями с ИИ для защиты корпоративных систем. Также она адресована руководителям IT-отделов, которые разрабатывают стратегии кибербезопасности, и data-аналитикам, работающим с большими данными и системами на базе ИИ. Важно, что курс также подходит для профессионалов технического или физико-математического профиля, стремящихся расширить

свою квалификацию в области информационной безопасности и искусственного интеллекта. Программа подходит как для повышения квалификации, так и для карьерного перехода.

Ф. Требования к уровню подготовки поступающего на обучение

Участники программы должны иметь техническое образование в области физико-математических наук, информационных технологий или смежных дисциплин, базовые знания в области компьютерных сетей, основ программирования и работы с базами данных.

Знание основ машинного обучения или искусственного интеллекта будет являться преимуществом.

Г. Продолжительность и форма обучения

Продолжительность обучения составляет 144 часа, из которых 80 часов контактных.

Форма обучения – очно-заочная, с использованием дистанционных технологий и электронного обучения.

При реализации программы с применением электронного обучения дистанционных образовательных технологий организация, осуществляющая образовательную деятельность, обеспечивает защиту информации ограниченного доступа.

Совершенствование профессиональных компетенций обеспечивается широким использованием в учебном процессе активных и интерактивных форм проведения занятий (компьютерных симуляций, разбора конкретных ситуаций) с целью развития профессиональных навыков обучающихся.

Программа повышения квалификации предусматривает проведение занятий в соответствии с целевыми установками, которые обеспечивают требуемый уровень усвоения учебного материала. Знания приобретаются на лекциях, семинарах и в ходе самостоятельной работы.

Н. Требования к материально-техническому обеспечению

Наличие у каждого слушателя компьютера и телефона с доступом в Интернет, микрофон, видеокамера.

И. Формы аттестации и оценочные материалы

Освоение программы повышения квалификации завершается обязательной итоговой аттестацией, в качестве задания итоговой аттестации предполагается подготовка презентации, в которой будет предложен проект по интеграции ИИ в систему информационной безопасности типичной компании отрасли работы, учитывая данные, с которыми она работает, и требования к защите и соблюдению этических норм. Проект предполагает интеграцию ИИ в систему информационной безопасности компании, ориентируясь на защиту данных и соблюдение этических норм.

Лицам, успешно освоившим программу повышения квалификации и прошедшим итоговую аттестацию, выдается удостоверение о повышении квалификации.

III. ОСНОВНОЕ СОДЕРЖАНИЕ ПРОГРАММЫ

А. Содержание учебных модулей

Программа охватывает все ключевые аспекты использования искусственного интеллекта в кибербезопасности. Она начинается с изучения основ ИИ, машинного обучения и нейронных сетей, а затем переходит к практическим вопросам, таким как методы защиты данных и анализ киберугроз. Особое внимание уделяется выявлению и предотвращению атак, включая социальную инженерию и фишинговые атаки, поддерживаемые ИИ.

Также программа охватывает защиту ИИ-систем от угроз, интеграцию ИИ в системы безопасности и этические аспекты работы с данными. Завершается курс проектной работой, где слушатели разрабатывают и защищают комплексное решение по кибербезопасности.

Программа не только предоставляет теоретическую базу, но и акцентируется на практическом применении знаний в современных цифровых экосистемах.

Разработанная программа включает 9 модулей, в каждом из которых предусмотрены лекции, практические занятия, и самостоятельная работа, которые проводятся с использованием системы дистанционного обучения ВУЗа.

Модуль 1 охватывает ключевые аспекты взаимодействия технологий искусственного интеллекта (ИИ) с мерами информационной безопасности. Учащиеся изучают основы ИИ, включая машинное обучение и нейронные сети, а также методы защиты информации в условиях быстроразвивающейся цифровой среды. Занятия включают теоретические концепции, практические примеры и кейсы, что позволяет студентам осваивать навыки интеграции ИИ в системы безопасности и анализировать влияние ИИ на защиту данных.

Модуль 2 предполагает анализ киберугроз, связанных с внедрением и использованием технологий искусственного интеллекта. В его рамках студенты изучают типы угроз, включая атаки на данные, манипуляции моделями и уязвимости систем ИИ. Особое внимание уделяется методам выявления, оценки и предотвращения атак на ИИ-системы, а также разработке эффективных стратегий защиты. Курс включает практические занятия, в которых студенты применяют теоретические знания для анализа реальных инцидентов и разработки решений по повышению безопасности ИИ-приложений.

Модуль 3 направлен на изучение стратегий и технологий, применяемых для обеспечения безопасности данных в средах, использующих искусственный интеллект. Курс охватывает основные принципы защиты данных, включая шифрование, анонимизацию, а также методы контроля доступа и управления идентификацией. Практические упражнения позволяют студентам разрабатывать эффективные решения для защиты данных в различных приложениях ИИ.

Модуль 4 посвящен применению технологий искусственного интеллекта в области кибербезопасности для идентификации угроз и разработки стратегий защиты. Студенты изучают алгоритмы, используемые для классификации и предсказания атак, а также методы обработки и визуализации данных, которые помогают в интерпретации результатов. Практические задания включают применение ИИ для создания систем обнаружения вторжений и моделирования сценариев атак.

В модуле 5 рассматривается динамично развивающееся направление в кибербезопасности, где искусственный интеллект используется для манипуляции и обмана пользователей с целью получения несанкционированного доступа к информации. В рамках курса студенты изучают методики социальной инженерии, включая фишинг, преследовательские атаки и различные техники воздействия на психологию человека. Модуль также охватывает стратегии защиты и противодействия атакам социальной инженерии, включая образовательные программы, инженерные решения и новые технологии. Обучающиеся получают навыки выявления потенциальных угроз и применения методов защиты, а также осваивают роль человеческого фактора в системе безопасности.

Модуль 6 фокусируется на внедрении и эффективном использовании технологий искусственного интеллекта в различных аспектах защиты информации. Курс охватывает ключевые темы, такие как автоматизация мониторинга и защиты, обнаружения угроз, анализ уязвимостей, создание интеллектуальных систем мониторинга и реагирования на инциденты. Студенты изучают современные алгоритмы машинного обучения и глубокого обучения, которые применяются для улучшения процессов идентификации аномалий и предсказания потенциальных атак. Практические занятия включают разработку и тестирование собственных решений на основе ИИ, внедрение автоматизированных систем безопасности и анализ реальных кейсов. Курс также исследует взаимодействие между ИИ и другими технологиями, такими как блокчейн и облачные технологии, в контексте повышения уровня информационной безопасности.

Модуль 7 посвящен изучению методов и подходов, направленных на обеспечение безопасности систем искусственного интеллекта от различных типов атак и уязвимостей, и анализу устойчивости систем к атакам. Рассматриваются ключевые аспекты, включая анализ рисков с применением матрицы Mitre, идентификацию угроз, а также разработку и внедрение защитных механизмов на всех этапах жизненного цикла ИИ-систем. Студенты исследуют специфические виды атак на модели машинного обучения, такие как атаки с подменой данных, целенаправленные ошибки и манипуляции с использованием adversarial examples.

В рамках модуля рассматриваются стратегии повышения устойчивости ИИ-моделей к атакам, такие как регуляризация, обучение с учетом adversarial

примеров и методы трансферного обучения. Практические занятия предоставляют возможность студентам создавать и тестировать защитные решения, а также анализировать реальные случаи атак на системы ИИ.

В рамках 8 модуля рассматриваются современные тренды и перспективы применения технологий искусственного интеллекта в области защиты информации и киберзащиты. Модуль охватывает ключевые аспекты, такие как автоматизация процессов управления безопасностью, использование машинного обучения для анализа угроз, прогнозирование атак и реагирование на инциденты. Студенты знакомятся с актуальными методами и инструментами, которые позволяют улучшить реакцию на кибератаки и эффективность защиты информационных систем. Также рассматриваются новые вызовы и препятствия, связанные с внедрением ИИ в кибербезопасность, например, уязвимость ИИ-моделей, правовые аспекты. Практические занятия и кейсы дают возможность студентам анализировать реальные сценарии использования ИИ в киберзащите и разрабатывать собственные решения для повышения безопасности.

Заключительный, 9, модуль посвящен исследованию этических вопросов, связанных с разработкой, внедрением и использованием технологий искусственного интеллекта. В рамках модуля рассматриваются основные концепции и теории этики, такие как утилитаризм, деонтология и др., и их применение к современным вызовам, возникающим в сфере ИИ. Студенты изучают ключевые темы, включая предвзятость алгоритмов, приватность данных, ответственность за решения, принимаемые ИИ-системами, а также влияние ИИ на общество и рабочие процессы. Здесь акцентируется внимание на важности создания этически обоснованных технологий и разработке стандартов их использования, а также на необходимости учета социокультурных контекстов при внедрении ИИ в различные сферы жизни. Практические занятия и дискуссии помогут студентам развить критическое мышление и сформировать собственную позицию по этическим вопросам.

В. Методические материалы и рекомендации

Теоретическая часть курса реализуется в рамках лекций, где обучающиеся изучают основные понятия, концепции и подходы к применению искусственного интеллекта (ИИ) в информационной безопасности. На лекциях излагаются наиболее важные и сложные темы, такие как принципы ИИ и машинного обучения, анализ киберугроз, использование и защита данных. Важным элементом является использование активных методов обучения.

При проведении занятий применяются различные методики:

- Введение в занятия (метод – проблемное обучение).

Занятие начинается с реальной проблемы, связанной с ИИ и информационной безопасностью, например, с вопроса: «Какие уязвимости могут возникнуть при использовании ИИ в банковской сфере?» Это создает мотивацию для изучения темы.

Практика предполагает использование тематических примеров и видеоматериалов, демонстрирующих потенциальные угрозы и решения на базе ИИ. Затем обсуждение идей и вариантов их решения в формате мозгового штурма.

- Разбор теории через практические примеры (метод кейсов).

Студенты получают конкретный кейс, например, анализ угроз для конкретной ИИ-системы в компании. Задача студентов — разобрать кейс в группах, предложить возможные решения и обсудить их с преподавателем.

При проведении практики каждой группе предлагается составить презентацию своих решений с указанием плюсов и минусов, применимых технологий и этических аспектов.

- Групповая работа и симуляции (командное обучение).

Студенты организуются в группы, каждая из которых выполняет часть большого задания, связанного с информационной безопасностью. Например, одна группа разрабатывает меры защиты данных, другая — анализирует потенциальные угрозы, третья — разрабатывает этическую политику по работе с данными.

- Практическое обсуждение текущих кейсов (дебаты и ролевые игры).

При проведении занятий используется метод дебатов для обсуждения спорных тем, например, этики использования ИИ. Это поможет учащимся видеть разные точки зрения и аргументировать свои позиции.

Для проведения практики формируются две команды. Одна группа отстаивает необходимость полного автоматизированного анализа данных в ИБ, другая — защиту конфиденциальности данных сотрудников и клиентов.

- Работа с примерами на практике и рефлексия (критическое мышление и рефлексия).

Завершаются занятия рефлексией: можно предложить студентам обсудить, какие аспекты изученной темы показались наиболее трудными, сделать выводы по результатам работы над кейсами, а также предоставить каждому участнику возможность озвучить, какие аспекты нужно улучшить в проекте и почему.

Практические занятия организуются для углубления и закрепления знаний, развития умений анализа информации и участия в дискуссиях, акцент делается на формирование и развитие навыков применения изученных методов для решения профессиональных задач в области информационной безопасности. Отличительной чертой разработанной программы является уникальный подход к обучению, который сочетает теорию, практику и интерактивные форматы работы. Она предполагает использование методики командных заданий с элементами игрового моделирования. Это позволяет не только изучить угрозы и защитные механизмы, но и ощутить себя на месте реальных киберконфликтов.

Практические работы выполняются в командах. Для этого обучающиеся делятся на команды по 4-6 человек,

каждая команда выбирает тему условной организации или области (например, финансы, здравоохранение, IT и т.д.). Далее внутри каждой команды обучающиеся еще делятся на две группы: «Защитники» и «Атакующие» (или «Красная команда / Red Team» и «Синяя команда / Blue Team»).

Роль атакующих. Группа атакующих разрабатывает стратегии атаки, используя методы, описанные в модуле 2, сценарии фишинговых атак.

В командах в рамках практических работ обеспечивается постоянное взаимодействие и обмен идеями согласно следующим принципам:

- Атакующие и Защитники. В каждой команде группы атакующих и защитников постоянно обмениваются идеями, комментариями по поводу возможных атак и способов защиты. Это позволяет участникам почувствовать себя как в роли атакующих, так и в роли защищающих.

- Ротация ролей. Регулярно проводить ротацию ролей между атакующими и защитниками. Например, каждые две недели или после завершения очередного модуля, участники меняются ролями. Это помогает всем участникам лучше понять оба аспекта задачи и развить навыки как в атаке, так и в защите.

- Обсуждение и дебаты. Организовать регулярные обсуждения и дебаты между группами атакующих и защитников. Это позволяет участникам критически оценивать идеи друг друга, находить слабые места в стратегиях и предлагать улучшения.

Для итогового проекта в каждой команде группы защитников и атакующих объединяют результаты работ по всем модулям и разрабатывают комплексный проект по возможным атакам и способам защиты условной организации на основе ИИ. Итоговый проект должен включать анализ угроз и уязвимостей, разработанные модели ИИ для обнаружения и предотвращения атак, меры защиты от социальной инженерии, интеграцию всех разработанных решений в единую систему защиты информации.

Презентация итогового проекта должна включать: описание выбранной области и условной организации, анализ угроз и уязвимостей, разработанные модели ИИ и меры защиты, интеграцию решений в единую систему защиты информации, результаты тестирования и оптимизации, выводы и рекомендации.

Общая максимальная сумма баллов при оценивании за все критерии составляет 100 баллов. В качестве критериев оценивания используются:

- Качество и полнота презентации, включая ясность и структурированность (0-10), полноту информации (0-10), визуальное оформление (0-5).
- Реалистичность и эффективность разработанных решений: реалистичность (0-10), эффективность (0-10), техническая осуществимость (0-5).
- Оригинальность и креативность решений: оригинальность (0-10), креативность (0-10).
- Интеграция всех разработанных решений в единую систему защиты информации: координация решений (0-10), единство системы (0-10).

- Убедительность и аргументированность ответов на вопросы: убедительность (0-5), аргументированность (0-5).

Для целей текущего контроля знаний в ходе занятий используются различные приемы контроля успеваемости обучающихся.

Самостоятельная работа организуется в рамках отведенного времени по заданиям, соответствующим тематике модуля. Обучающиеся выполняют задания, направленные на развитие аналитического и критического мышления (например, изучение публикаций и составление обзора по современным тенденциям использования ИИ в информационной безопасности, сбор данных из открытых источников для последующего анализа, составление отчета по текущим требованиям к защите персональных данных и этическим аспектам использования ИИ). В ходе самостоятельной работы обучающиеся получают консультации у преподавателей.

С. Методика организации проектно-соревновательной деятельности

Цель соревнования – продемонстрировать навыки и стратегии в области информационной безопасности с акцентом на использование искусственного интеллекта (ИИ). Команды атаки пытаются обойти системы защиты, используя ИИ-технологии, а команды защиты стремятся предотвратить атаки, также применяя ИИ. Соревнования проходят на инфраструктуре промышленного партнера или инфраструктуре обучающей площадки (реализация на датасетах и синтетических данных, системах моделирования, а также на клиент-серверных приложениях).

Формат соревнования – командная работа с ограниченным временем.

Примеры кейсов

Кейс 1. Финансовый сектор.

Атака – генерация *adversarial examples* для обмана моделей машинного обучения, используемых в системах обнаружения мошенничества.

Защита – разработка и внедрение систем обнаружения аномалий на основе ИИ для выявления и нейтрализации *adversarial examples*.

Кейс 2. Здравоохранение.

Атака – манипуляция данными в системах хранения медицинских записей с целью кражи конфиденциальной информации.

Защита – шифрование данных и реализация политик безопасности для доступа к медицинским записям с использованием ИИ для анализа и предотвращения несанкционированных действий.

Шкала оценивания:

35-40 баллов. Высокая эффективность атак/защиты, творческий подход, убедительная презентация.

25-34 балла. Удовлетворительная эффективность атак/защиты, средний уровень креативности, хорошая презентация.

15-24 балла. Низкая эффективность атак/защиты, ограниченный креативный подход, слабая презентация.

Менее 15 баллов. Неэффективные атаки/защита, отсутствие креативного подхода, плохая презентация.

D. Методика выбора стека технологий и массивов данных

Основываясь на уровне подготовки студентов, определяется стек технологий, соответствующий их профессиональной деятельности и навыкам. Например, для базового уровня подойдут инструменты, такие как Google Colab, ELK Stack, SQL.

Получаемые навыки, такие как умение работать с массивами данных, анализировать сетевой трафик и тестировать простые ИИ-моделей, подбираются в зависимости от задач компаний, где работают студенты.

Рекомендации по выбору технологий:

1. Для работы с данными: Python (пакеты pandas, Scikit-learn) для обработки и анализа данных.

2. Для визуализации и мониторинга: Matplotlib, Seaborn и инструменты визуализации в реальном времени, такие как ELK Stack, для отслеживания показателей безопасности.

3. Для предсказательного анализа: простые модели в Scikit-learn, использование Snort и Wireshark для анализа сетевого трафика и обнаружения угроз.

Выбор массивов данных:

1. Учебные наборы данных по информационной безопасности такие как NSL-KDD или MITRE ATT&CK, которые содержат данные об атаках и уязвимостях.

2. Реальные и открытые данные. Использование журналов активности и сетевых данных (анонимизированных), чтобы адаптировать результаты к реальной среде компании.

3. Отраслевые данные. Студенты могут использовать данные из корпоративных источников, если это соответствует нормам безопасности компании, или же использовать открытые наборы данных из Kaggle, которые подходят для обучения и тестирования ИИ-моделей.

IV. ЗАКЛЮЧЕНИЕ

По итогам деятельности рабочей группы, в которую вошли представители шести ВУЗов (Воронеж, Муром, Чебоксары, Москва) была разработана программа повышения квалификации «Искусственный интеллект и кибербезопасность: защита данных в цифровую эпоху», основная цель которой — подготовка специалистов, способных адаптироваться к быстро меняющимся условиям в сфере кибербезопасности и активно внедрять инновационные технологии для защиты информации. В рамках разработанного курса также рассматриваются новые вызовы и препятствия, связанные с внедрением ИИ в кибербезопасность, такие как уязвимости ИИ-моделей, этические вопросы и правовые аспекты. Практические занятия и кейс-стадии дают возможность обучающимся анализировать реальные сценарии использования ИИ в киберзащите и разрабатывать собственные решения для повышения безопасности.

Разработанная программа повышения квалификации отличается от существующих российских аналогов более высоким уровнем интеграции компетенций в области искусственного интеллекта и

кибербезопасности, системной опорой на нормативные и профессиональные документы, а также акцентом на практико-ориентированную и проектную подготовку специалистов.

БИБЛИОГРАФИЯ

- [1] Zhai, Y., Yan, J., Zhang, H., and Lu, W. (2020). Tracing the evolution of AI: conceptualization of artificial intelligence in mass media discourse. *Inform. Discov. Deliv.* 48, 137–149. doi: 10.1108/IDD-01-2020-0007
- [2] Ziems N., Wu S. Security Vulnerability Detection Using Deep Learning Natural Language Processing, *IEEE INFOCOM 2021 IEEE Conference on Computer Communications Workshops*, 2021, pp. 1–6
- [3] Молодяков С. А. Применение нейронных сетей для обработки мультимедийного контента (100 примеров на Python) : монография / Санкт-Петербург : ПОЛИТЕХ-ПРЕСС, 2025 572 с. doi: 10.18720/SPBPU/2/id25-4.
- [4] Evsutin O., Melman A., Meshcheryakov R. Digital steganography and watermarking for digital images: a review of current research directions *IEEE Access*. 2020. Vol. 8, pp. 166589–166611.
- [5] Крыжановский В. Д., Крыжановская Ю. А. Применение нейронной сети для решения задачи классификации в судебной медицине. *Вестник УрФО. Безопасность в информационной сфере*. Челябинск, 2023; 3 (49): 21-27. DOI: 10.14529/secur230302.
- [6] Munkhdalai, L., Munkhdalai, T., Namsrai, O., Lee, J., Ryu, K. (2019). An Empirical Comparison of Machine-Learning Methods on Bank Client Credit Assessments. *Sustainability*, 11(3), 699. doi: 10.3390/su11030699.
- [7] Shanthi, R.R., Sasi, N.K., and Gouthaman, P. (2023). A new era of cybersecurity: the influence of artificial intelligence. *2023 international conference on networking and communications (ICNWC)*, Chennai, India. pp. 1–4
- [8] Donepudi P. K. (2015). Crossing Point of Artificial Intelligence in Cybersecurity. *American Journal of Trade and Policy*, 2(3), 121-128. <https://doi.org/10.18034/ajtp.v2i3.493>
- [9] Wang, Yang & McCoe, Margaret & Hu, Qian & Jalalitar, Maryam. (2024). Teaching Security in the Era of Generative AI: A Course Design of Security + ChatGPT. 01-06. 10.1109/ISEC61299.2024.10664905.
- [10] Alotaibi A., Rassam M.A. Adversarial Machine Learning Attacks Against Intrusion Detection Systems: A Survey on Strategies and Defense. *Future Internet*. 2023. Vol. 15. No. 2. P. 62. DOI: 10.3390/fi15020062
- [11] D. Codetta-Raiteri and L. Portinale, "Decision Networks for Security Risk Assessment of Critical Infrastructures," *ACM Trans. Internet Technol.*, vol. 18, no. 3, pp. 1–22, 2018.
- [12] D. Ippoliti, C. Jiang, Z. Ding, and X. Zhou, "Online Adaptive Anomaly Detection for Augmented Network Flows," *ACM Trans. Auton. Adapt. Syst.*, vol. 11, no. 3, pp. 17:1–17:28, 2016.
- [13] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," *IEEE Trans. Emerg. Top. Comput. Intell.*, vol. 2, no. 1, pp. 41–50, 2018.
- [14] Y. Du, J. Wang, and Q. Li, "An android malware detection approach using community structures of weighted function call graphs," *IEEE Access*, vol. 5, pp. 17478–17486, 2017.
- [15] Sarker, Iqbal & Furhad, Md & Nowrozy, Raza. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN Computer Science*. 2. 10.1007/s42979-021-00557-0.
- [16] Котенко И.В., Мельник М.В. Применение гибридной нейронной сети AE-LSTM для обнаружения аномалий в контейнерных системах // *Известия ЮФУ. Технические науки*. 2024. № 5 (241). С. 38-47. DOI: 10.18522/2311-3103-2024-5-38-47 // <https://elibrary.ru/item.asp?id=77817442>
- [17] Ebert, Christof & Beck, Maximilian. (2023). Artificial Intelligence for Cybersecurity. *IEEE Software*. 40. 27-34. 10.1109/MS.2023.3305726.
- [18] Mazurczyk, Wojciech & Lee, Dongwon & Vlachos, Andreas. (2024). Disinformation 2.0 in the Age of AI: A Cybersecurity Perspective. *Communications of the ACM*. 67. 36-39. 10.1145/3624721.
- [19] Muheidat, Fadi & Mallouh, Moayyad & Al-Saleh, Omar & Al-Khasawneh, Omar & Tawalbeh, Lo'ai. (2024). Applying AI and Machine Learning to Enhance Automated Cybersecurity and Network Threat Identification. *Procedia Computer Science*. 251. 287-294. 10.1016/j.procs.2024.11.112.
- [20] Salem, Aya & Azzam, Safaa & Emam, O. & Abohany, Amr. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data*. 11. 10.1186/s40537-024-00957-y.
- [21] Vulpe, Simona & Rughinis, Razvan & Turcanu, Dinu & Rosner, Daniel. (2024). AI and cybersecurity: a risk society perspective. *Frontiers in Computer Science*. 6. 10.3389/fcomp.2024.1462250.
- [22] Сухомлин, В. А. Архитектура и принципы разработки курса для дисциплины «Кибербезопасность» / В. А. Сухомлин, О. С. Белякова, А. С. Климина, М. С. Полянская, Е. В. Зубарева, А. В. Якушин. – DOI 10.25559/SIPITO.16.202004.927-939 // *Современные информационные технологии и ИТ-образование*. – 2020. – Т. 16, No 4. – С. 927-939.
- [23] Сухомлин, В. А. Создание профиля «Кибербезопасность и искусственный интеллект» для направления подготовки ФИИТ на основе куррикулумного подхода / В. А. Сухомлин. – DOI 10.25559/SIPITO.17.202103.724-734 // *Современные информационные технологии и ИТ-образование*. – 2021. – Т. 17, No 3. – С. 724-734
- [24] Arış, Ahmet & Puche Rondon, Luis & Ortiz, Daniel & Ross, Monique & Finlayson, Mark & Uluagac, Selcuk. (2022). Integrating Artificial Intelligence into Cybersecurity Curriculum: New Perspectives. 10.18260/1-2–41761.
- [25] Serik, M. (2024). Improving the content of the special course "Information Security" during the training process: detecting cyber attacks using machine learning. *Journal of Educational Sciences*. 78. 10.26577/JES20247801015.
- [26] Alomar, Ban & Trabelsi, Zouheir & Qayyum, Tariq & Ambali Pambil, Medha Mohan. (2024). AI and Network Security Curricula: Minding the Gap. 1-7. 10.1109/EDUCON60312.2024.10578588.

Professional Development Program Elaboration: "Artificial Intelligence and Cybersecurity: Digital Age Data Protection"

Y. A. Kryzhanovskaya, N. V. Dorofeev, A. V. Khristoforova, T. A. Nikolaev, T. V. Mitrofanova,
V.Y. Gerasin, O.I. Ashirova

Abstract — Alfa Bank and ITMO University initiated and implemented the "Modern Artificial Intelligence in Higher Education" program In the past, 2024-2025, academic year. In this article the final project - professional development program "Artificial Intelligence and Cybersecurity: Digital Age Data Protection", completed by a developers team, representing six universities in Voronezh, Kazan, Moscow, Murom, and Cheboksary is presented. As a preliminary step, similar existing solutions analysis was carried out, It made possible to substantiate presented program structure and content. The program is designed for those professionals who seeking not only for their knowledge in information security expanding but also for master modern artificial intelligence technologies for data protection. The program combines three main areas: studying the AI fundamentals and its application in cybersecurity, practical work on identifying and preventing threats using AI, and analyzing the ethical and legal using AI technologies aspects. It provides a theoretical foundation and emphasizes the practical application of knowledge in modern digital ecosystems also. The program key aim is to train specialists who can effectively apply AI to solve monitoring, analyzing and preventing attacks issues in the modern digital challenges face. The program's format emphasizes teamwork, allowing participants to immerse themselves in real-world threat scenarios and develop their practical skills. The outcome is a comprehensive project in which teams pool their expertise to develop solutions to protect a simulated corporate system, taking into account modern AI technologies and cyber threats. Elaborated program is suitable for both professional development and career advancement.

Keywords — cybersecurity, artificial intelligence, professional development, training methods

REFERENCES

- [1] Zhai, Y., Yan, J., Zhang, H., and Lu, W. (2020). Tracing the evolution of AI: conceptualization of artificial intelligence in mass media discourse. *Inform. Discov. Deliv.* 48, 137–149. doi: 10.1108/IDD-01-2020-0007
- [2] Ziems N., Wu S. Security Vulnerability Detection Using Deep Learning Natural Language Processing, *IEEE INFOCOM 2021 IEEE Conference on Computer Communications Workshops*, 2021, pp. 1–6
- [3] Molodykov S. A. Applications of Neural Networks for Multimedia Processing: 100 Python Examples. St. Petersburg: POLYTECHPRESS, 2025, 572 p. (In Russ.) Available at: 10.18720/SPBPU/2/id25-4.
- [4] Evsutin O., Melman A., Meshcheryakov R. Digital steganography and watermarking for digital images: a review of current research directions *IEEE Access*. 2020, Vol. 8, pp. 166589–166611.
- [5] Kryzhanovskii V. D., Kryzhanovskaya Yu. A. Solving Classification Issue in Forensic Examination: Neural Network Application. *Journal of the Ural Federal District. Information security*. 2023; 3(49): 21-27. (In Russ.) DOI: 10.14529/secur230302.
- [6] Munkhdalai, L., Munkhdalai, T., Namsrai, O., Lee, J., Ryu, K. (2019). An Empirical Comparison of Machine-Learning Methods on Bank Client Credit Assessments. *Sustainability*, 11(3), 699. doi: 10.3390/su11030699.
- [7] Shanthi, R.R., Sasi, N.K., and Gouthaman, P. (2023). A new era of cybersecurity: the influence of artificial intelligence. 2023 international conference on networking and communications (ICNWC), Chennai, India, pp. 1–4
- [8] Donepudi P. K. (2015). Crossing Point of Artificial Intelligence in Cybersecurity. *American Journal of Trade and Policy*, 2(3), 121-128. <https://doi.org/10.18034/ajtp.v2i3.493>
- [9] Wang, Yang & McCoey, Margaret & Hu, Qian & Jalalitar, Maryam. (2024). Teaching Security in the Era of Generative AI: A Course Design of Security + ChatGPT. 01-06. 10.1109/ISEC61299.2024.10664905.
- [10] Alotaibi A., Rassam M.A. Adversarial Machine Learning Attacks Against Intrusion Detection Systems: A Survey on Strategies and Defense. *Future Internet*. 2023. Vol. 15. No. 2. P. 62. DOI: 10.3390/fi15020062
- [11] D. Codetta-Raiteri and L. Portinale, "Decision Networks for Security Risk Assessment of Critical Infrastructures," *ACM Trans. Internet Technol.*, vol. 18, no. 3, pp. 1–22, 2018.
- [12] D. Ippoliti, C. Jiang, Z. Ding, and X. Zhou, "Online Adaptive Anomaly Detection for Augmented Network Flows," *ACM Trans. Auton. Adapt. Syst.*, vol. 11, no. 3, pp. 17:1–17:28, 2016.
- [13] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," *IEEE Trans. Emerg. Top. Comput. Intell.*, vol. 2, no. 1, pp. 41–50, 2018.
- [14] Y. Du, J. Wang, and Q. Li, "An android malware detection approach using community structures of weighted function call graphs," *IEEE Access*, vol. 5, pp. 17478–17486, 2017.
- [15] Sarker, Iqbal & Furhad, Md & Nowrozy, Raza. (2021). AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. *SN Computer Science*. 2. 10.1007/s42979-021-00557-0.
- [16] Котенко И.В., Мельник М.В. Применение гибридной нейронной сети AE-LSTM для обнаружения аномалий в контейнерных системах // *Известия ЮФУ. Технические науки*. 2024. № 5 (241). С. 38-47. DOI: 10.18522/2311-3103-2024-5-38-47 // <https://elibrary.ru/item.asp?id=77817442>
- [17] Ebert, Christof & Beck, Maximilian. (2023). Artificial Intelligence for Cybersecurity. *IEEE Software*. 40. 27-34. 10.1109/MS.2023.3305726.
- [18] Mazurczyk, Wojciech & Lee, Dongwon & Vlachos, Andreas. (2024). Disinformation 2.0 in the Age of AI: A Cybersecurity Perspective. *Communications of the ACM*. 67. 36-39. 10.1145/3624721.
- [19] Muheibat, Fadi & Mallouh, Moayyad & Al-Saleh, Omar & Al-Khasawneh, Omar & Tawalbeh, Lo'ai. (2024). Applying AI and Machine Learning to Enhance Automated Cybersecurity and Network Threat Identification. *Procedia Computer Science*. 251. 287-294. 10.1016/j.procs.2024.11.112.
- [20] Salem, Aya & Azzam, Safaa & Emam, O. & Abohany, Amr. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data*. 11. 10.1186/s40537-024-00957-y.
- [21] Vulpe, Simona & Rughinis, Razvan & Turcanu, Dinu & Rosner, Daniel. (2024). AI and cybersecurity: a risk society perspective. *Frontiers in Computer Science*. 6. 10.3389/fcomp.2024.1462250.
- [22] Sukhomlin V.A., Belyakova O.S., Klimina A.S., Polyanskaya M.S., Zubareva E.V., Yakushin, A.V. Architecture and Principles of Developing a Curriculum for the Academic Subject "Cybersecurity". *Sovremennye informacionnye tehnologii i IT-obrazovanie = Modern Information Technologies and IT-Education*. 2020; 16(4):927-939. DOI: <https://doi.org/10.25559/SITITO.16.202004.927-939>
- [23] Sukhomlin V.A. Creating a Profile "Cybersecurity and Artificial Intelligence" for the Direction of FIIT Training Based on the

Curriculum Approach. Sovremennye informacionnye tehnologii i IT-obrazovanie = Modern Information Technologies and IT-Education. 2021; 17(3):724-734. DOI: <https://doi.org/10.25559/SITITO.17.202103.724-734>

- [24] Arış, Ahmet & Puche Rondon, Luis & Ortiz, Daniel & Ross, Monique & Finlayson, Mark & Uluagac, Selcuk. (2022). Integrating Artificial Intelligence into Cybersecurity Curriculum: New Perspectives. 10.18260/1-2--41761.
- [25] Serik, M. (2024). Improving the content of the special course "Information Security" during the training process: detecting cyber attacks using machine learning. Journal of Educational Sciences. 78. 10.26577/JES20247801015.
- [26] Alomar, Ban & Trabelsi, Zouheir & Qayyum, Tariq & Ambali Parambil, Medha Mohan. (2024). AI and Network Security Curricula: Minding the Gap. 1-7. 10.1109/EDUCON60312.2024.10578588.

About the authors:

Yuliana A. Kryzhanovskaya, senior lector, Information Systems Cybersecurity chair, computer software chair, Applied Mathematics, Informatics and Mechanics Faculty, Voronezh State University (1 Universitetskaya pl., Voronezh, 394018, Russia), ORCID: <https://orcid.org/0000-0002-7420-1900>, jak@mail.ru

Nikolai V. Dorofeev, Head of the Department of Management and Control in Technical Systems, Vladimir State University (23, Orlovskaya Street, Murom, Vladimir Region, 602264, Russia), Doctor of Technical

Sciences, ORCID: <https://orcid.org/0000-0002-1636-7654>, dorofeevny@yandex.ru

Anastasiia V. Khristoforova, Associate Professor of the Department of Mathematical and Hardware Support for Information Systems, Federal State Budgetary Educational Institution of Higher Education "Chuvash State University named after I.N. Ulyanov" (15, Moskovsky Prospekt, Cheboksary, Chuvash Republic, 428015, Russia), Cand. Sc. (Physics and Mathematics), ORCID: <https://orcid.org/0000-0003-3534-8747>, dlya.nastenki@mail.ru

Timur A. Nikolaev, Senior Lecturer, Department of Information Technology and Security, Timiryasov Kazan Innovative University, (42 Moskovskaya St, Kazan, 420111, Republic of Tatarstan, Russia), ORCID: <https://orcid.org/0000-0002-5410-2278>, timur_nikolaev@inbox.ru

Tatiana V. Mitrofanova, Associate Professor of the Department of Mathematical and Hardware Support for Information Systems, Federal State Budgetary Educational Institution of Higher Education "Chuvash State University named after I.N. Ulyanov" (15, Moskovsky Prospekt, Cheboksary, Chuvash Republic, 428015, Russia), Cand. Sc. (Physics and Mathematics), ORCID: <https://orcid.org/0000-0002-5750-7991>, mitrofanova_tv@mail.ru

Vladislav Y. Gerasin, teacher, Federal State Budgetary Educational Institution of Higher Education «RTU MIREA College of Programming and Cybersecurity» (78 Vernadsky Avenue, Moscow, 119454, Russia), ORCID: <https://orcid.org/0009-0001-9748-2047>, gerasin.vladislav@mail.ru

Oksana I. Ashirova, Master of Economics, Department of Regional Economics and Geography, Faculty of Economics, Peoples' Friendship University of Russia (6 Miklukho-Maklaya Street, Moscow, 117198, Russia), ORCID: 0009-0006-8656-3366, ashirova-oi@pfur.ru