

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Баламирзоев Назим Лиодинович
Должность: Ректор
Дата подписания: 02.05.2026 10:44:07
Уникальный идентификатор документа:
5cf0d6f89e80f49a334f6a4ba58e91f3326b9926

Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Дагестанский государственный технический университет»

ПРОГРАММА ПРАКТИЧЕСКОЙ ПОДГОТОВКИ В ФОРМЕ ПРЕДДИПЛОМНОЙ ПРАКТИКИ

для направления подготовки 10.04.01 Информационная безопасность
код и полное наименование направления подготовки

по направленности Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта

факультет Компьютерных технологий и энергетики
наименование факультета, где ведется дисциплина

кафедра Информационная безопасность и программная инженерия
наименование кафедры, за которой закреплена дисциплина

Форма обучения очная курс 2 семестр (ы) 4
очная

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность с учетом рекомендаций и ОПОП ВО по направлению подготовки и программе магистратуры «Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта»

Разработчик 
(подпись)

Качаева Г.И., к.э.н.
(ФИО уч. степень, уч. звание)

« 02 » февраля 2026 г.

Зав. кафедрой, за которой закреплена дисциплина


(подпись)

Качаева Г.И., к.э.н.
(ФИО уч. степень, уч. звание)

« 03 » февраля 2026 г.

Программа одобрена на заседании выпускающей кафедры информационной безопасности и программной инженерии от « 05 » февраля 2026 года, протокол № 6/1

Зав. выпускающей кафедрой по данному направлению подготовки

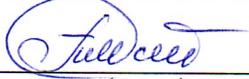

(подпись)

Качаева Г.И. к.э.н.
(ФИО уч. степень, уч. звание)

« 05 » февраля 2026 г.

Программа одобрена на заседании Методического совета факультета компьютерных технологий и энергетики от « 10 » февраля 2026 г., протокол № 5/1

Председатель Методического совета факультета КТиЭ


(подпись)

Исабекова Т.И., к.ф.-м.н., доцент
(ФИО уч. степень, уч. звание)

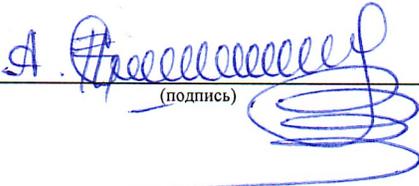
« 10 » февраля 2026 г.

Декан факультета 
(подпись)

Т.А. Рагимова
(ФИО)

Начальник УО 
(подпись)

Л.Н. Мусаева
(ФИО)

Проректор по УР 
(подпись)

А.Ф. Демирова
(ФИО)

СОДЕРЖАНИЕ

1. Общая характеристика программы преддипломной практики.....	4
1.1. Цели и задачи преддипломной практики.....	4
1.2. Место преддипломной практики в структуре ОПОП.....	4
1.3.Формы проведения преддипломной практики.....	5
1.4. Место и время проведения преддипломной практики	6
1.5. Планируемые результаты освоения преддипломной практики.....	6
2. Структура и содержание преддипломной практики.....	8
2.1. Объем программы отводимый на освоение практики.....	8
2.2. Содержание преддипломной практики	8
2.3. Формы отчетности по преддипломной практики	9
3. Условия реализации программы преддипломной практики.....	10
3.1. Материально-техническое обеспечение	10
3.2. Учебно-методическое и информационное обеспечение программы.....	10
3.2.1. Печатные издания	10
3.2.2. Основные электронные издания	11
4. Контроль и оценка результатов освоения преддипломной практики.....	13

1. Общая характеристика программы преддипломной практики

1.1. Цели и задачи преддипломной практики

Целью преддипломной практики является завершение подготовки выпускной квалификационной работы (далее – ВКР) (магистерской диссертации), включая окончательное оформление текста, апробацию результатов исследования и подготовку к процедуре защиты.

Задачами преддипломной практики являются:

- завершение разработки и экспериментальной апробации моделей, методов или алгоритмов в области киберразведки и противодействия угрозам с применением технологий искусственного интеллекта;
- окончательная обработка, анализ и систематизация результатов научного исследования;
- доработка текста выпускной квалификационной работы в соответствии с требованиями нормативной документации и стандартов университета;
- подготовка и оформление графического, демонстрационного и презентационного материала для защиты ВКР;
- подготовка доклада для выступления на заседании государственной экзаменационной комиссии;
- проверка объема заимствований и обеспечение оригинальности текста ВКР;
- подготовка к публичной защите результатов исследования.

1.2. Место преддипломной практики в структуре ОПОП

Преддипломная практика является обязательным разделом ОПОП ВО и представляет собой вид учебных занятий, ориентированных на практическую проектную деятельность.

Прохождение практики базируется на знаниях и компетенциях, сформированных в результате освоения следующих дисциплин учебного плана: Защищенные информационные системы, Технологии обеспечения информационной безопасности, Управление информационной безопасностью, Интеллектуальные системы и технологии, Технологии извлечения знаний из больших данных, Библиотеки машинного обучения, Технологии машинного обучения в кибербезопасности, Управление проектами интеллектуальных информационных систем, Правовое регулирование сферы искусственного интеллекта и интеллектуальной собственности, Теория обнаружения вторжений с применением искусственного интеллекта, Системы мониторинга и управления инцидентами информационной безопасности, Методы сбора и обработки данных из открытых источников, Система для сбора событий и логов, Принятие решений на основе проактивного поиска и обнаружения угроз, Интеллектуальные системы информационной безопасности в промышленных системах, Оценка достоверности источников информации.

Для освоения данной практики обучающемуся необходимо:

Знать:

- современное состояние и тенденции развития методов киберразведки, обнаружения вторжений и противодействия компьютерным атакам;
- теоретические основы и алгоритмы интеллектуальных систем, технологий машинного обучения и глубокого обучения, применяемых для решения задач информационной безопасности;
- архитектуру, принципы функционирования и методы защиты информационных систем различного назначения;
- методы сбора, предобработки и анализа больших данных, включая данные из открытых источников, сетевой трафик, системные логи и события;

- нормативную и правовую базу в области информационной безопасности, защиты интеллектуальной собственности и правового регулирования искусственного интеллекта;
- методологию научного исследования, планирования эксперимента, статистической обработки данных и оценки эффективности разработанных решений;
- требования к структуре, содержанию и оформлению выпускных квалификационных работ, а также правила подготовки научных публикаций.

Уметь:

- формулировать цель, задачи, научную новизну и практическую значимость исследования в предметной области;
- осуществлять критический анализ проблемных ситуаций, выявлять уязвимости и векторы атак, обоснованно выбирать методы и средства защиты;
- разрабатывать и программно реализовывать модели и алгоритмы искусственного интеллекта для задач кибербезопасности с использованием современных библиотек и фреймворков;
- проводить вычислительные эксперименты, оценивать качество полученных моделей по метрикам, интерпретировать и визуализировать результаты;
- работать с профессиональными базами данных научной литературы и патентной информации, систематизировать и критически оценивать источники;
- оформлять отчеты о научно-исследовательской работе, научные статьи, тезисы докладов и иную техническую документацию;
- использовать инструменты проверки объема заимствований и обеспечения оригинальности текста.

Владеть:

- навыками самостоятельного планирования и проведения научно-исследовательской деятельности в области киберразведки и противодействия угрозам с применением искусственного интеллекта;
- методами обработки и анализа структурированных и неструктурированных данных с использованием языков программирования (Python, SQL) и специализированных библиотек (scikit-learn, PyTorch, TensorFlow, pandas, NumPy);
- технологиями проектирования и эксплуатации систем обнаружения вторжений, мониторинга инцидентов, сбора и корреляции событий;
- навыками подготовки и публичной защиты результатов исследования, включая создание презентационных материалов и докладов;
- инструментарием для оценки достоверности информации и верификации источников данных;
- практическими приемами оформления текста выпускной квалификационной работы в соответствии с требованиями ГОСТ и вуза

Данная практика закрепляет и развивает компетенции в области: киберразведки и проактивного поиска угроз информационной безопасности; обнаружения вторжений и анализа защищенности объектов информатизации с применением технологий искусственного интеллекта; сбора, обработки и корреляции событий и логов из разнородных источников; мониторинга и управления инцидентами информационной безопасности; применения методов машинного обучения и интеллектуальных систем для выявления аномалий и компьютерных атак; оценки достоверности информации и верификации источников данных; проектирования, разработки и эксплуатации систем защиты информации в различных отраслях (промышленность, здравоохранение); организации и

проведения научных исследований, оформления и публичной защиты результатов интеллектуальной деятельности; подготовки, оформления и защиты выпускной квалификационной работы.

1.3. Формы проведения преддипломной практики

Преддипломная практика проводится в следующей форме:

- непрерывно – путем выделения в графике учебного процесса непрерывного периода учебного времени для проведения всех видов практик, предусмотренных ОПОП ВО.

1.4. Место и время проведения преддипломной практики

Местом прохождения практики является выпускающая кафедра, а также профильные организации: АО «Завод «Дагдизель», Федеральное казенное учреждение «Центр инженерно-технического обеспечения и вооружения управления федеральной службы исполнения наказаний по Республике Дагестан».

Преддипломная практика проводится сроком 8 недель, 432 часа.

Способы проведения практики: выездная.

Способы проведения практики, предусмотренной ОПОП ВО, устанавливаются выпускающей кафедрой с учетом требований ФГОС ВО.

1.5. Планируемые результаты освоения преддипломной практики

В результате освоения преддипломной практики обучающийся должен овладеть следующими компетенциями:

Таблица 1.

Код и наименование компетенции	Код и наименование индикаторов достижения компетенции
ПК- 1 Способен разрабатывать и применять процедуры и интеллектуальные средства информационно-аналитических систем поддержки принятия решений по обеспечению информационной безопасности	ПК- 1.1 Способен решать задачи анализа данных в целях обеспечения информационной безопасности
	ПК- 1.2 Способен интерпретировать и использовать результаты решения информационно-аналитических задач безопасности
	ПК- 1.3 Способен разрабатывать информационно-аналитические системы в сфере информационной безопасности
ПК-2 Способен выполнять мониторинг и ситуационный анализ обстановки в сфере информационной безопасности	ПК -2.1 Способен формализовывать задачи информационно-аналитической поддержки принятия решений в сфере информационной безопасности
	ПК-2.2 Способен разрабатывать процедуры мониторинга обстановки в сфере информационной безопасности
ПК-3 Способен исследовать и разрабатывать архитектуры систем искусственного интеллекта для различных предметных областей на основе комплексов методов и инструментальных средств систем искусственного интеллекта	ПК-3.1 Выбирает комплексы методов и инструментальных средств искусственного интеллекта для решения задач в зависимости от особенностей предметной области
ПК-4 Способен разрабатывать и	ПК-4.1 Ставит задачи по разработке или

применять методы и алгоритмы машинного обучения для решения задач искусственного интеллекта	совершенствованию методов и алгоритмов для решения комплекса задач предметной области
	ПК-4.2 Разрабатывает унифицированные и обновляет методологии описания, сбора и разметки данных, а также механизмы контроля за соблюдением указанных методологий
ПК -5 Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях	ПК-5.1 Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях
ПК-6 Способен выбирать, разрабатывать и проводить экспериментальную проверку работоспособности программных компонентов систем искусственного интеллекта по обеспечению требуемых критериев эффективности и качества функционирования	ПК-6.1 Выбирает и разрабатывает программные компоненты систем искусственного интеллекта
	ПК-6.2 Проводит экспериментальную проверку работоспособности систем искусственного интеллекта
ПК-7 Способен руководить проектами по созданию комплексных систем искусственного интеллекта	ПК-7.1 Руководит разработкой искусственного интеллекта
ПК-8 Способен руководить проектами по созданию, поддержке и использованию систем искусственного интеллекта на основе нейросетевых моделей и методов	ПК-8.1 Руководит работами по оценке и выбору моделей искусственных нейронных сетей и инструментальных средств для решения поставленных задач

2. Структура и содержание преддипломной практики

2.1. Объем программы отводимый на освоение практики

Преддипломная практика проводится в 4 семестре.

Всего: 12 з.е. / 432 часа.

Продолжительность практики: 8 недель.

Промежуточная аттестация в форме зачет с оценкой.

2.2. Содержание преддипломной практики

Таблица 2.

Разделы (этапы) практики	Коды компетенций, формированию которых способствует элемент программы	Виды работ обучающегося на практике	Количество часов	Формы текущего контроля
Организационно-подготовительный этап	ПК-1: ПК-1.1, ПК-1.2, ПК-1.3; ПК-2: ПК-2.1, ПК-2.2, ПК-3: ПК-3.1; ПК-4: ПК-4.1, ПК-4.2; ПК-5: ПК-5.1; ПК-6: ПК-6.1, ПК-6.2; ПК-7: ПК-7.1; ПК-8: ПК-8.1	Участие в установочной конференции, прохождение инструктажа по технике безопасности. Получение индивидуального задания от руководителя практики. Уточнение темы выпускной квалификационной работы, корректировка плана-графика выполнения ВКР. Составление индивидуального плана прохождения практики.	20	Собеседование с руководителем. Утверждение индивидуального плана
Завершение научно-исследовательской работы и доработка ВКР	ПК-1: ПК-1.1, ПК-1.2; ПК-2: ПК-2.1, ПК-2.2; ПК-4: ПК-4.1; ПК-6: ПК-6.1, ПК-6.2; ПК-8: ПК-8.1	Проведение завершающих экспериментов, тестирования разработанных моделей и алгоритмов. Доработка программной реализации (при наличии). Обработка и статистический анализ полученных результатов. Формулирование окончательных выводов и положений научной новизны. Оформление практической главы ВКР.	150	Промежуточные консультации. Проверка руководителем текста глав ВКР, результатов экспериментов, исходного кода
Оформление выпускной квалификационной работы	ПК-1: ПК-1.3; ПК-4: ПК-4.2; ПК-5: ПК-5.1	Окончательное оформление текста ВКР в соответствии с требованиями ГОСТ и нормативной документации университета. Подготовка и оформление графического материала, схем, таблиц, приложений. Проверка объема заимствований	120	Проверка текста ВКР на соответствие требованиям. Справка о результатах проверки на антиплагиат. Заключение

		(антиплагиат). Прохождение нормоконтроля. Оформление списка использованных источников.		нормоконтролера
Подготовка к защите ВКР	ПК-3: ПК-3.1, ПК-7: ПК-7.1	Подготовка текста доклада для выступления на заседании ГЭК. Разработка презентации и раздаточного материала. Репетиция защиты с руководителем. Участие в предзащите на выпускающей кафедре. Устранение замечаний, полученных в ходе предзащиты.	100	Предзащита ВКР на кафедре. Проверка презентации и доклада
Итоговая аттестация по практике	ПК-1: ПК-1.1, ПК-1.2, ПК-1.3; ПК-2: ПК-2.1, ПК-2.2, ПК-3: ПК-3.1; ПК-4: ПК-4.1, ПК-4.2; ПК-5: ПК-5.1; ПК-6: ПК-6.1, ПК-6.2; ПК-7: ПК-7.1; ПК-8: ПК-8.1	Подготовка и оформление отчета по преддипломной практике, дневника практики. Защита отчета перед руководителем / комиссией кафедры. Получение зачет с оценкой.	42	Защита отчета. Зачет с оценкой
Итого за семестр			432	

2.3. Формы отчетности по преддипломной практике

Итоги работы по каждому разделу (этапу) преддипломной практики по мере их завершения подводятся в форме собеседования. К итоговой аттестации в конце практики составляется и защищается отчет по практике, в итоге руководитель практики выставляет зачет с оценкой. Отчет по практике должен содержать следующие разделы (ориентировочный объем каждого раздела – 1–3 стр.):

Введение (содержит описание целей, задач и объектов изучения);

Теоретические вопросы (изложение вопросов, рассмотренных на теоретических занятиях);

Практические вопросы (описание выполненных учебных (практических) работ);

Результаты работы (представляются результаты обработки и анализа полученной информации);

Список использованных источников литературы.

3. Условия реализации программы преддипломной практики

3.1. Материально-техническое обеспечение

Обучающиеся для прохождения преддипломной практики направляются на следующие организации Республики Дагестан:

Акционерное общество «Завод «Дагдизель»:

Управление завода, кабинет № 228.

Программное и программно-аппаратное обеспечение: рабочие станции Windows (7-10-11); маршрутизаторы; коммутаторы; Windows server 2025 Data center); СУДБ (PostgreSQL, MySQL); межсетевой экран; средства защиты информации; доменные службы; системы резервного копирования; антивирусы: Kaspersky, Dr.Web.

Федеральное казенное учреждение «Центр инженерно-технического обеспечения и вооружения управления федеральной службы исполнения наказаний по Республике Дагестан»:

Мастерская по ремонту и настройке инженерно-технических средств охраны и надзора, средств связи, компьютерная и оргтехника, аппаратные средства: средства защиты информации от не санкционированного доступа СЗИ от НСД, аппаратно-программный комплекс шифрования данных АПКШ, средства криптографической защиты информации СКЗИ;

Программные средства: антивирусное программное обеспечение, СЭД УИС, АРМ ГС, мессенджер «ЗИМБРА», СТАТ ОПЕРАТОР, АКУС УИС, ИСПКД, СЭМПЛ).

3.2. Учебно-методическое и информационное обеспечение программы

Для реализации программы библиотечный фонд образовательной организации имеет печатные и/или электронные образовательные и информационные ресурсы для использования в образовательном процессе. При формировании библиотечного фонда образовательной организации выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список может быть дополнен новыми изданиями

3.2.1. Печатные издания

Основная литература:

1. Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения / А. И. Белоус, В. А. Солoduха. — Москва: Техносфера, 2021. — 482 с. — ISBN 978-5-94836-612-8. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/108023.html>
2. Платонов, В. В. Технологии машинного обучения в кибербезопасности: учебное пособие / В. В. Платонов. — Москва, Вологда: Инфра-Инженерия, 2024. — 140 с. — ISBN 978-5-9729-2048-8. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/144586.html>
3. Зенков, А. В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст: электронный // ЭБС «Лань». — URL: <https://e.lanbook.com/book/308945>.
4. Джоши, П. Машинное обучение и безопасность / П. Джоши. — Москва: ДМК Пресс, 2023. — 282 с. — ISBN 978-5-93700-119-3. — Текст: электронный // ЭБС «IPR BOOKS». — URL: <https://www.iprbookshop.ru/120212.html>.

5. Менисов, А. Б. Кибершит. Искусственный интеллект и кибербезопасность / А. Б. Менисов. — Москва, Алматы: Ай Пи Ар Медиа, EDP Hub (Идипи Хаб), 2024. — 166 с. — ISBN 978-5-4497-2336-9. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/138398.html>
6. Мюллер, А. Введение в машинное обучение с помощью Python. Руководство для специалистов по работе с данными / А. Мюллер, С. Гвидо. — Москва: ДМК Пресс, 2022. — 480 с. — ISBN 978-5-93700-109-4. — Текст: электронный // ЭБС «IPR BOOKS». — URL: <https://www.iprbookshop.ru/112358.html>.
7. Шолмов, Л. Ю. Киберразведка и анализ угроз: практическое руководство / Л. Ю. Шолмов. — Москва: БХВ-Петербург, 2024. — 304 с. — ISBN 978-5-9775-4200-1. — Текст: электронный // ЭБС «Лань». — URL: <https://e.lanbook.com/book/325112>.
8. Распопов, Р. В. Управление проектами в сфере информационных технологий: учебник и практикум для вузов / Р. В. Распопов. — Москва: Издательство Юрайт, 2024. — 297 с. — (Высшее образование). — ISBN 978-5-534-18002-2. — Текст: электронный // ЭБС «Лань». — URL: <https://e.lanbook.com/book/322478>

Дополнительные источники:

1. Менисов, А. Б. Технологии искусственного интеллекта и кибербезопасность : монография / А. Б. Менисов. — Москва: Ай Пи Ар Медиа, 2022. — 133 с. — ISBN 978-5-4497-1788-7. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/123570.html>
2. Журавлев, Е. В. Анализ больших данных в информационной безопасности / Е. В. Журавлев. — Москва: Горячая линия–Телеком, 2023. — 198 с. — ISBN 978-5-9912-0887-8. — Текст: электронный // ЭБС «IPR BOOKS». — URL: <https://www.iprbookshop.ru/121456.html>.
3. Рассказова, П. А. Машинное обучение на Python: классификация, кластеризация и выявление аномалий / П. А. Рассказова. — Москва: ДМК Пресс, 2024. — 340 с. — ISBN 978-5-93700-130-8. — Текст: электронный // ЭБС «IPR BOOKS». — URL: <https://www.iprbookshop.ru/125678.html>.
4. Белов, Е. Б. Основы информационной безопасности: учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. — Москва: Горячая линия–Телеком, 2006. — 544 с. — ISBN 5-93517-307-3. — Текст: электронный // ЭБС «Лань». — URL: <https://e.lanbook.com/book/45567>.
5. Черемушкин, А. В. Криптографические протоколы: учебное пособие / А. В. Черемушкин. — Москва: Издательство Юрайт, 2023. — 156 с. — ISBN 978-5-534-16543-2. — Текст: электронный // ЭБС «Лань». — URL: <https://e.lanbook.com/book/310112>
6. Велигура, А. Н. Комбинаторика и теория графов для кибербезопасности. Конспект лекций: учебное пособие / А. Н. Велигура. — Москва: Национальный исследовательский ядерный университет «МИФИ», 2021. — 200 с. — ISBN 978-5-7262-2836-5. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/125492.html>

3.2.2. Основные электронные издания

1. Python Software Foundation. Python 3 Official Documentation. — URL: <https://docs.python.org/3/>.
2. NumPy Community. NumPy User Guide. — URL: <https://numpy.org/doc/stable/user/index.html>.

3. pandas Development Team. pandas Documentation. — URL: <https://pandas.pydata.org/docs/>.
4. scikit-learn Developers. scikit-learn User Guide. — URL: https://scikit-learn.org/stable/user_guide.html.
5. MITRE. MITRE ATT&CK® — матрица тактик и техник кибератак. — URL: <https://attack.mitre.org/>.
6. «Информационная безопасность» (журнал). — URL: <https://www.itsec.ru/>. — Режим доступа: по подписке через ЭБС «Лань» (при наличии).
7. CNews: Безопасность. Интернет-издание о высоких технологиях и ИБ. — URL: <https://safe.cnews.ru/>.
8. GCHQ. CyberChef — инструмент для анализа и декодирования данных. — URL: <https://gchq.github.io/CyberChef/>.
9. «Безопасность информационных технологий». Научный журнал, входящий в Перечень ВАК. Издаётся НИЯУ МИФИ. — URL: <https://bit.spels.ru/>. — Режим доступа: по подписке через ЭБС «Лань».
10. «Вопросы кибербезопасности». Научный журнал категории К1 в Перечне ВАК. — URL: <https://cyberrus.info/>. — Режим доступа: по подписке через ЭБС «IPRbooks».
11. arXiv.org. Open access archive of scholarly articles. — URL: <https://arxiv.org/>.
12. IEEE Xplore Digital Library. — URL: <https://ieeexplore.ieee.org/Xplore/home.jsp>. — Режим доступа: по подписке вуза.
13. Российский индекс научного цитирования (РИНЦ) на платформе eLibrary.ru. — URL: <https://elibrary.ru/>. — Режим доступа: по подписке вуза.
14. University of California, Irvine. UCI Machine Learning Repository. — URL: <https://archive.ics.uci.edu/>.
15. Kaggle, Inc. Kaggle Datasets. — URL: <https://www.kaggle.com/datasets>.
16. Canadian Institute for Cybersecurity (CIC). Intrusion Detection Datasets (CIC-IDS). — URL: <https://www.unb.ca/cic/datasets/index.html>.
17. Диогенес, Ю. Кибербезопасность: стратегии атак и обороны / Ю. Диогенес, Э. Озкая; перевод Д. А. Беликов. — Москва: ДМК Пресс, 2020. — 326 с. — ISBN 978-5-97060-709-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/124557.html>

4. Контроль и оценка результатов освоения преддипломной практики

Контроль и оценка результатов освоения преддипломной практики осуществляется руководителем практики в процессе проведения практики, самостоятельного выполнения обучающимися индивидуальных заданий, выполнения практических работ.

Результаты обучения	Формы и методы контроля и оценки
Проявляет готовность к планированию, командной работе и деловой коммуникации в профессиональной среде.	Наблюдение за работой в организации. Анализ дневника практики, содержащего описание ежедневных задач, процесса взаимодействия с коллективом и стейкхолдерами. Оценка вклада в работу проектной команды.
Владеет методами управления проектом: формирует задачу, разрабатывает план, осуществляет мониторинг и корректировку.	Проверка и оценка проектной документации: Устава проекта, Иерархической структуры работ, детального календарного плана-графика, протоколов совещаний.
Демонстрирует способность оформлять результаты профессиональной деятельности в виде полного пакета проектной и технической документации.	Проверка и оценка качества, структуры, ясности и полноты итогового отчета по практике, а также сопутствующих документов (техническое предложение, руководства, описание API).
Владеет профессиональной терминологией, понимает принципы организации защищенной ИТ-инфраструктуры предприятия и соблюдает ее регламенты.	Устный опрос в ходе консультаций. Анализ характеристики от руководителя практики с места ее прохождения. Оценка учета требований ИБ при проектировании.
Применяет системный подход и фундаментальные знания для анализа задачи, выбора и обоснования технологического стека, методов и архитектурных решений.	Защита технического предложения или эскизного проекта. Оценка глубины аналитического отчета, обоснованности выбранных инструментов, алгоритмов и архитектуры разрабатываемого решения.
Способен реализовать проектное решение: разрабатывать программный код, настраивать среды, интегрировать компоненты.	Проверка работоспособности прототипа или скриптов. Анализ исходного кода, комментариев, логики реализации. Контроль умения работать с системами контроля версий и средствами контейнеризации.
Владеет методами тестирования, валидации и оценки эффективности технологических решений.	Анализ раздела отчета, содержащего описание тестов, полученных метрик, выводов об эффективности и безопасности решения.
Применяет алгоритмы и технологии машинного обучения для решения прикладных задач в области информационной безопасности и киберразведки.	Оценка практической части работы: корректности выбора, реализации, обучения и настройки моделей машинного обучения; качества подготовки и обработки данных; интерпретации результатов работы модели в контексте задач ИБ.
Способен организовать завершающий этап проекта: подготовить решение к передаче, провести презентацию результатов, сформировать итоговые выводы.	Защита итогового проекта. Оценка полноты итогового пакета документов, готовности решения к внедрению и качества итоговой отчетности.

Специальные условия инвалидам и лицам с ограниченными возможностями здоровья (ОВЗ)

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Специальные условия обучения и направления работы с инвалидами и лицами с ОВЗ определены на основании:

- Федерального закона от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»;
- Федерального закона от 24.11.1995 № 181-ФЗ «О социальной защите инвалидов в Российской Федерации»;
- приказа Минобрнауки России от 06.04.2021 № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры»;
- методических рекомендаций по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса, утвержденных Минобрнауки России 08.04.2014 № АК-44/05вн).

Под специальными условиями для получения образования обучающихся с ОВЗ понимаются условия обучения, воспитания и развития, включающие в себя использование при необходимости адаптированных образовательных программ и методов обучения и воспитания, специальных учебников, учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего необходимую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания ДГТУ и другие условия, без которых невозможно или затруднено освоение ОПОП обучающихся с ОВЗ.

Обучение в рамках учебной дисциплины обучающихся с ОВЗ осуществляется ДГТУ с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Обучение по учебной дисциплине обучающихся с ОВЗ может быть организовано как совместно с другими обучающимися, так и в отдельных группах.

В целях доступности обучения по дисциплине обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

- наличие альтернативной версии официального сайта ДГТУ в сети «Интернет» для слабовидящих;
- весь необходимый для изучения материал, согласно учебному плану (в том числе, для обучающихся по индивидуальным учебным планам) предоставляется в электронном виде на диске.
- индивидуальное равномерное освещение не менее 300 люкс;
- присутствие ассистента, оказывающего обучающемуся необходимую помощь;
- обеспечение возможности выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);
- обеспечение доступа обучающегося, являющегося слепым и использующего собаку-проводника, к зданию ДГТУ.

2) для лиц с ОВЗ по слуху:

- наличие микрофонов и звукоусиливающей аппаратуры коллективного пользования (аудиоколонки);

3) для лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата, материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов и других приспособлений).

Перед началом обучения могут проводиться консультативные занятия, позволяющие студентам с ОВЗ адаптироваться к учебному процессу.

В процессе ведения учебной дисциплины научно-педагогическим работникам рекомендуется использование социально-активных и рефлексивных методов обучения, технологий социокультурной реабилитации с целью оказания помощи обучающимся с ОВЗ в установлении полноценных межличностных отношений с другими обучающимися, создании комфортного психологического климата в учебной группе.

Особенности проведения текущей и промежуточной аттестации по дисциплине для обучающихся с ОВЗ устанавливаются с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и др.). При необходимости предоставляется дополнительное время для подготовки ответа на зачете или экзамене.