Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет имени В.А. Бондаренко»

Кафедра компьютерной безопасности и математического обеспечения информационных систем

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.В.Э.6.1 Основы промпт-инжиниринга»

Уровень высшего образования

СПЕЦИАЛИТЕТ

Специальность
10.05.01 Компьютерная безопасность
(код и наименование специальности)

специализация №3 «Разработка защищенного программного обеспечения»
(наименование направленности (профиля)/специализации образовательной программы)

Квалификация
Специалист по защите информации

Форма обучения
Очная

Год набора 2026

Рабочая программа дисциплины «*Б1.Д.В.Э.6.1 Основы промпт-инжиниринга*» рассмотрена и утверждена на заседании кафедры

Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры

протокол № 9 от "20" марта 2026 г.

Заведующий кафедрой
Кафедра компьютерной безопасности и математического обеспечения информационных систем
наименование кафедры *подпись* И.В. Влацкая *расшифровка подписи*

Исполнители:
доцент *должность* *подпись* К.Р. Джукашев *расшифровка подписи*

должность подпись
расшифровка подписи

СОГЛАСОВАНО:
Председатель методической комиссии по специальности
10.05.01 Компьютерная безопасность *код наименование* *личная подпись* И.В. Влацкая *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
личная подпись С.А. Биктимирова *расшифровка подписи*

Уполномоченный по качеству института
личная подпись С.Н. Морозова *расшифровка подписи*

№ регистрации _____

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

Формирование у обучающихся теоретических знаний и практических навыков в области промпт-инжиниринга применительно к задачам обеспечения компьютерной безопасности, а также развитие компетенций, необходимых для проектирования защищённых систем информатизации с использованием технологий генеративного искусственного интеллекта (LLM).

Задачи:

1. Изучить принципы работы больших языковых моделей (LLM) и их архитектурные особенности с точки зрения безопасности.
2. Освоить методы и техники промпт-инжиниринга для решения профессиональных задач в области защиты информации.
3. Сформировать умения выявлять и анализировать уязвимости, связанные с промпт-инженерингом (промпт-инъекции, джейлбрейки, утечка контекста).
4. Научить проектировать безопасные промпты и разрабатывать защитные механизмы для систем, использующих LLM.
5. Привить навыки интеграции LLM и промпт-инжиниринга в процессы анализа защищённости, реагирования на инциденты и автоматизации задач компьютерной безопасности.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к дисциплинам (модулям) по выбору вариативной части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.В.3 Разработка и применение систем искусственного интеллекта*

Постреквизиты дисциплины: *Отсутствуют*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ПК*-1 Проектирование объектов в защищенном исполнении	ПК*-1-В-1 Умеет проектировать средства и системы информатизации в защищенном исполнении ПК*-1-В-2 Владеет навыками проектирования систем защиты информации на объектах информатизации	**Знать:** принципы построения защищённых систем с использованием LLM; классификацию угроз, связанных с промпт-инжинирингом; методы формализации требований к промптам; нормативно-методическую базу применения ИИ в системах защиты

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
		информации; модели угроз для LLM-компонентов. **Уметь:** разрабатывать архитектуру безопасного взаимодействия с LLM; выбирать и настраивать модели для задач защиты информации; проектировать промпты, устойчивые к атакам; интегрировать LLM в SIEM/SOC-процессы; разрабатывать защитные фильтры и санитайзеры для пользовательских промптов. **Владеть:** методиками тестирования промптов на безопасность; навыками документирования решений по защите систем с LLM; навыками построения систем предотвращения промпт-инъекций; приёмами мониторинга и аудита взаимодействия с LLM.

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 академических часов).

Вид работы	Трудоемкость, академических часов	
	9 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**68,25**	**68,25**
Лекции (Л)	34	34
Лабораторные работы (ЛР)	34	34
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- выполнение индивидуального творческого задания (ИТЗ);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- изучение разделов курса в системе электронного обучения;*	**39,75**	**39,75**

Вид работы	Трудоемкость, академических часов	
	9 семестр	всего
- изучение разделов массового открытого онлайн-курса; *- подготовка к лабораторным занятиям)*		
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**зачет**	

Разделы дисциплины, изучаемые в 9 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Введение в промпт-инжиниринг и LLM	16	4		4	8
2	Промпт-инжиниринг для задач кибербезопасности	18	6		4	8
3	Уязвимости и атаки на основе промптов	22	8		6	8
4	Методы защиты и безопасный промпт-дизайн	22	8		6	8
5	Интеграция LLM в системы защиты информации	30	8		14	8
	Итого:	108	34		34	40
	Всего:	108	34		34	40

4.2 Содержание разделов дисциплины

1. Введение в промпт-инжиниринг и LLM. Основные понятия: промпт, LLM, токенизация, внимание, генерация. Архитектуры: трансформеры, GPT, LLaMA, Claude. Парадигмы взаимодействия: zero-shot, few-shot, chain-of-thought. Роль промпт-инжиниринга в компьютерной безопасности.

2. Промпт-инжиниринг для задач кибербезопасности. Применение LLM для анализа логов, трафика, кода на уязвимости. Автоматическое написание отчётов по безопасности. Генерация правил для IDS/IPS. Разработка сценариев для SOAR. Техники few-shot для классификации вредоносных событий.

3. Уязвимости и атаки на основе промптов. Классификация атак: промпт-инъекции (прямые и косвенные), джейлбрейки, утечка промпта, токенизационные атаки, атаки на контекстное окно. Анализ реальных кейсов (ChatGPT, Bing, Llama). Методики реверс-инжиниринга системных промптов.

4. Методы защиты и безопасный промпт-дизайн. Принципы безопасного промптинга: изоляция пользовательского ввода, использование разделителей, фильтрация вывода. Санитайзеры, выходные фильтры, детекция инъекций на основе LLM. Ролевые модели (RBAC) для доступа к LLM. Шаблоны защищённых промптов.

5. Интеграция LLM в системы защиты информации. Проектирование защищённых систем с LLM: обработка конфиденциальных данных, шифрование контекста, анонимизация. Примеры: LLM-агенты для SOC, автоматизированные пентестеры, системы анализа защищённости кода. Правовые и этические аспекты использования ИИ в кибербезопасности.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Знакомство с LLM и базовыми промптами	4
2	2	Использование LLM для анализа кода на уязвимости	4
3	3	Моделирование атак промпт-инъекций	6
4	4	Разработка защитного фильтра для промптов	6
5	5	Интеграция LLM в SIEM-систему	6
6	5	Комплексное проектирование защищённого LLM-агента	8
		Итого:	34

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Робототехника и искусственный интеллект : учебник для вузов / П. А. Лукин, Я. М. Машуков, Д. В. Романов, В. В. Тимофеев. — 2-е изд., стер. — Санкт-Петербург : Лань, 2026. — 128 с. — ISBN 978-5-507-51196-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/507449 (дата обращения: 15.04.2026). — Режим доступа: для авториз. пользователей.

2. Программирование, тестирование, проектирование, нейросети, технологии аппаратно-программных средств (практические задания и способы их решения) : учебник : [16+] / С. В. Веретехина, К. С. Кармицкий, Д. Д. Лукашин [и др.]. – Москва : Директ-Медиа, 2022. – 144 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=694782 (дата обращения: 15.04.2026). – Библиогр. в кн. – ISBN 978-5-4499-3321-8. – DOI 10.23681/694782. – Текст : электронный.

5.2 Дополнительная литература

1. Применение инструментов искусственного интеллекта в учебной и профессиональной деятельности : учебно-методическое пособие / Н. И. Исупова, Н. А. Бояринцева, Е. А. Мамаева [и др.]. — Киров : ВятГУ, 2025. — 117 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/516165 (дата обращения: 15.04.2026). — Режим доступа: для авториз. пользователей.

2. Боровская, Е. В. Основы искусственного интеллекта : учебное пособие : [16+] / Е. В. Боровская, Н. А. Давыдова. – 6-е изд. – Москва : Лаборатория знаний, 2024. – 130 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=718135 (дата обращения: 15.04.2026). – Библиогр. в кн. – ISBN 978-5-93208-797-8. – Текст : электронный.

5.3 Периодические издания

1. Вестник компьютерных и информационных технологий: журнал. - М. : ООО "Издательский дом "Спектр" — URL: https://www.vkit.ru/
2. Программные продукты и системы : журнал. - Научно-исследовательский институт «Центр-программсистем» (г. Тверь) — URL: https://www.swsys.ru/.

5.4 Интернет-ресурсы

1. https://openedu.ru/course/hse/PROMPT_ENGINEERING/ / - «Открытое образование», Каталог курсов, МООК: «Введение в промпт-инжиниринг»

2. https://openedu.ru/course/spbu/AIoT - «Открытое образование», Каталог курсов, МООК: «Применение искусственного интеллекта в системах интернета вещей»

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система РЕД ОС.
2. Пакет офисных приложений «МойОфис Образование»
3. Для работы с ресурсами Интернет - веб-браузер Яндекс https://yandex.ru/..
4. ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990–2026]. – Режим доступа в сети ОГУ http://garant.net.osu.ru
5. Автоматизированная интерактивная система сетевого тестирования - АИССТ (зарегистрирована в РОСПАТЕНТ, Свидетельство о государственной регистрации программы для ЭВМ №2011610456, правообладатель – Оренбургский государственный университет), режим доступа - http://aist.osu.ru.

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, семинарского типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения лабораторных занятий компьютерный класс, оснащенный компьютерами с операционной системой Astra Linux текущей версии с установленным пакетом офисных программ и интегрированной средой разработки ПО.

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к сети "Интернет", и обеспечением доступа в электронную информационно-образовательную среду ОГУ.