Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина Система для сбора событий и логов
наименование дисциплины по ОПОП

для направления подготовки 10.04.01 Информационная безопасность
код и полное наименование направления

по направленности Кибеpразведка 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) 3
очная

г. Махачкала – 2026

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 «Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта»

Разработчик _____ Мирземагомедова М.М., к.т.н.
(подпись) (ФИО уч. степень, уч. звание)

« 02 » февраля 2026 г.

Зав. кафедрой, за которой закреплена дисциплина

_____ Качаева Г.И., к.э.н.
(подпись) (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

_____ Качаева Г.И. к.э.н.
(подпись) (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

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

« 10 » февраля 2026 г.

Декан факультета _____ Т.А. Рагимова
(подпись) (ФИО)

Начальник УО _____ Л.Н. Мусаева
(подпись) (ФИО)

Проректор по УР _____ А.Ф. Демирова
(подпись) (ФИО)

Содержание

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ 4
1.1. Место дисциплины в структуре ОПОП 4
1.2. Цели и задачи освоения дисциплины 4
1.3. Компетенции обучающегося, формируемые в результате освоения дисциплины 4
2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ 5
2.1. Объем дисциплины и виды учебной работы 5
2.2. Содержание дисциплины 6
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ 9
3.1. Материально-техническое обеспечение 9
3.2. Учебно-методическое и информационное обеспечение программы 9
3.2.1. Печатные издания 10
3.2.2. Основные электронные издания 10
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ 11

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

1.1. Место дисциплины в структуре ОПОП

Дисциплина «Система для сбора событий и логов» входит в часть, формируемую участниками образовательных отношений учебного плана по программе магистратуры 10.04.01 Информационная безопасность, направленность «Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта»

Предшествующими дисциплинами, формирующими начальные знания, являются: Технологии обеспечения информационной безопасности, Защищенные информационные системы, Библиотеки машинного обучения, Технологии машинного обучения в кибербезопасности, Теория обнаружения вторжений с применением искусственного интеллекта, Управление информационной безопасностью, Интеллектуальные системы и технологии, Специальные разделы математики.

Дисциплина «Система для сбора событий и логов» является основополагающей для изучения следующих дисциплин: Принятие решений на основе проактивного поиска и обнаружения угроз, Производственная (проектно-технологическая) практика, Преддипломная практика, Государственная итоговая аттестация.

1.2. Цели и задачи освоения дисциплины

Дисциплина «Система для сбора событий и логов» способствует формированию у обучающихся компетенций, предусмотренных данной рабочей программой в соответствии с требованиями ФГОС ВО и ОПОП ВО по направлению подготовки 10.04.01 Информационная безопасность с учетом специфики направленности подготовки «Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта».

1.3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины «Система для сбора событий и логов» обучающийся должен овладеть следующими компетенциями:

Таблица 1.

Код и наименование компетенции	Код и наименование индикаторов достижения компетенции
ПК-2 Способность выполнять мониторинг и ситуационный анализ обстановки в сфере информационной безопасности	ПК-2.2 Способен разрабатывать процедуры мониторинга обстановки в сфере информационной безопасности
ПК-4 Способность разрабатывать и применять методы и алгоритмы машинного обучения для решения задач искусственного интеллекта	ПК-4.2 Разрабатывает унифицированные и обновляемые методологии описания, сбора и разметки данных, а также механизмы контроля за соблюдением указанных методологий
ПК-6 Способность 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

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем дисциплины и виды учебной работы

Таблица 2.

Вид учебной работы	**Форма обучения**
	очная
Объем образовательной программы дисциплины (ЗЕТ/ в часах)	3/108
В том числе:	**Объем в часах**
Лекции	17
Практические занятия	-
Лабораторные занятия	34
Самостоятельная работа	57
Курсовой проект (работа), семестр	-
Промежуточная аттестация в форме зачета**,** семестр	3 семестр
Часы на экзамен	-

2.2. Содержание дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций, формированию которых способствует элемент программы
1. Способы и методы машинного обучения для решения задач искусственного			
Тема 1.1 Способы машинного обучения	Обучение с учителем. Обучение без учителя. Обучение с частичным привлечением учителя. Обучение с подкреплением. Глубинное обучение.	**2**	ПК-2; ПК-4; ПК-6
	в том числе лабораторных занятий:	**4**	
	Лабораторная работа № 1. Практические методы предобработки данных на ЯП Python. Применение обучения с учителем, обучения без учителя, обучение с подкреплением.		
	Самостоятельная работа обучающихся: Интеграция с облачным многоэтапным конвейером анализа машинного обучения.	**8**	
Тема 1.2 Методы машинного обучения	1. Нейронные сети. 2. Дерево решений. 3. Метод случайного леса. 4. Кластеризация данных. Поиск ассоциативных правил.	**2**	ПК-2; ПК-4; ПК-6
	в том числе лабораторных занятий:	**4**	
	Лабораторная работа № 2. Нейронные сети. Дерево решений. Метод случайного леса. Кластеризация данных. Поиск ассоциативных правил.		
	Самостоятельная работа обучающихся: Применение нейронных сетей. Применение метода случайного леса.	**8**	

Тема 1.3 Многоуровневое машинное обучение для обнаружения продвинутых угроз ИБ	Обнаружение продвинутых угроз и вредоносных коммуникаций в ИКС. Интеграция с облачным многоэтапным конвейером анализа машинного обучения. Система анализа поведения пользователя и устройства для выявления вредоносных заражений, коммуникаций с командными серверами, утечки данных, а также потенциально нежелательных приложений, работающих в инфраструктуре ИКС.	**2**	ПК-2; ПК-4; ПК-6
	в том числе лабораторных занятий:	**4**	
	Лабораторная работа № 3. Интеграция с облачным многоэтапным конвейером анализа машинного обучения. Разработка системы анализа поведения пользователя.		
	Самостоятельная работа обучающихся: Использование ИКС для получения дополнительной контекстной информации об узле, имени пользователя, MAC-адресе устройств.	**8**	
Тема 1.4 Глобальные аналитические данные по угрозам	Глобальные аналитические данные по угрозам, создание дополнительного уровня защиты от бот-сетей и сложных атак. Корреляция подозрительной активности в ИКС.	**2**	ПК-2; ПК-4; ПК-6
	в том числе лабораторных занятий:	**4**	
	Лабораторная работа № 4. Создание дополнительного уровня защиты от бот-сетей. Разработка программы подсчета корреляции подозрительной активности в ИКС		
	Самостоятельная работа обучающихся: Использование ИКС для получения дополнительной контекстной информации об узле, имени пользователя, MAC-адресе устройств.	**8**	
2. Методы моделирования поведения и мониторинг обстановки в сфере информационной			
Тема 2.1 Моделирование поведения при внутренних угрозах	Обнаружение аномального поведения пользователей и подача сигнала тревоги о «сборе данных» или «утечке данных». Использование ИКС для получения дополнительной контекстной информации об узле, имени пользователя, MAC адресе устройств. Размещение подозрительных узлов сети в карантин.	**2**	ПК-2; ПК-4; ПК-6
	в том числе лабораторных занятий:	**4**	
	Лабораторная работа № 5. Имитация APT-атаки на домен. Имитация APT-атаки на linux-инфраструктуру.		
	Самостоятельная работа обучающихся: Обнаружение продвинутых угроз и вредоносных коммуникаций в ИКС.	**8**	

Тема 2.2 Создание системы сбора событий безопасности домена	Основные компоненты системы сбора событий безопасности домена. Журналирование событий в домене Active Directory. Выбор ЯП, библиотек для работы с машинным обучением	**2**	ПК-2; ПК-4; ПК-6
	в том числе лабораторных занятий:	**4**	
	Лабораторная работа № 6. Применение методов машинного обучения для обнаружения аномального поведения пользователей. Применение методов машинного обучения для обнаружения аномального поведения пользователей.		
	Самостоятельная работа обучающихся: Обнаружение продвинутых угроз и вредоносных коммуникаций в ИКС	**8**	
Тема 2.3 Реализация и мониторинг политик сегментации	Создание политики интеллектуальной сегментации для управления доступом к критически важным ресурсам. Критерии при сегментации ИКС.	**2**	ПК-2; ПК-4; ПК-6
	в том числе лабораторных занятий:	**4**	
	Лабораторная работа № 7. Критически важные ресурсы в ИКС организации. Создание политики интеллектуальной сегментации для управления доступом к критически важным ресурсам.		
	Самостоятельная работа обучающихся: Глубинное обучение.	**8**	
Тема 2.4 Создание системы сбора событий безопасности домена	Основные компоненты системы сбора событий безопасности домена. Журналирование событий в домене Active Directory. Выбор ЯП, библиотек для работы с машинным обучением.	**3**	ПК-2; ПК-4; ПК-6
	в том числе лабораторных занятий:	**6**	
	Лабораторная работа № 8. Парсинг журнала событий Security.evtx. Применение интеллектуального анализа для выявления аномального поведения пользователей домена		
	Самостоятельная работа обучающихся: Система анализа поведения пользователя и устройства для выявления вредоносных заражений, коммуникаций с командными серверами.	**1**	
Итого за 3 семестр:			
Лекции		**17**	
Лабораторные работы		**34**	
Самостоятельная работа		**57**	
Всего:		**108**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Материально-техническое обеспечение дисциплины «Система для сбора событий и логов» включает:

Наименование помещения	Перечень основного оборудования
Лаборатория защиты информации	Рабочее место преподавателя; Посадочные места по количеству обучающихся; Автоматизированные рабочие места (ПК в сборе) с доступом в сеть Интернет; Интерактивная система в составе: проектор интерактивная доска Программное и программно-аппаратное обеспечение: Лицензия на СУБД Tantor в редакции Special Edition, со встроенной полнофункциональной модульной платформой администрирования и мониторинга кластеров PostgreSQL «Тантор», на базе процессорной архитектуры x86-64, для сервера на 1 физическое или виртуальное ядро; ПАК «Мобильный носитель лицензий»; Служебный носитель «Секрет Особого Назначения» криптографический с быстрым процессором, 32Гб (арт. 620520); Elastic Stack, Graylog, Loki (Grafana); Fluentd, Logstash, Winlogbeat
Аудитория для проведения занятий лекционного типа	Рабочее место преподавателя; Посадочные места по количеству обучающихся; Автоматизированные рабочие места (ПК в сборе) с доступом в сеть Интернет; Интерактивная система в составе: проектор, интерактивная доска
Аудитория для самостоятельной работы обучающихся	Автоматизированные рабочие места (ПК в сборе) с доступом в сеть Интернет; Интерактивная система в составе: проектор, интерактивная доска

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. Тюгашев А. А. Интеллектуальные системы [Электронный ресурс]:учебное пособие. - Самара: СамГУПС, 2020. - 151 с. URL: https://e.lanbook.com/book/161308
2. Баланов, А. Н. Бэкенд-разработка веб-приложений: архитектура, проектирование и управление проектами : учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 312 с. URL: https://e.lanbook.com/book/394556
3. Штеренберг, С. И. Исследование проблем построения доверенной среды передачи : учебное пособие / С. И. Штеренберг, И. А. Ушаков, М. А. Скорых. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2024. — 121 с. URL: https://e.lanbook.com/book/426317

Дополнительные источники:

1. Баланов, А. Н. Комплексное руководство по разработке: от мобильных приложений до веб-технологий : учебное пособие для вузов / А. Н. Баланов. — Санкт-Петербург : Лань, 2024. — 412 с. — ISBN 978-5-507-48841-4. URL: https://e.lanbook.com/book/394577
2. Нестеров С. А. Основы информационной безопасности [Электронный ресурс]:учебное пособие. - Санкт-Петербург: Лань, 2019. - 324 с. URL: https://e.lanbook.com/book/114688

3.2.2. Основные электронные издания

1. COMSOL Multiphysics® ПО для мультифизического моделирования https://www.comsol.ru
2. Информационный портал Российского научного фонда http://www.rscf.ru
3. Российский фонд фундаментальных исследований https://www.rfbr.ru

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий.

Результаты обучения	**Критерии оценки**	**Методы оценки**
- Способен разрабатывать процедуры мониторинга обстановки в сфере информационной безопасности; - Разрабатывает унифицированные и обновляемые методологии описания, сбора и разметки данных, а также механизмы контроля за соблюдением указанных методологий; - Выбирает и разрабатывает программные компоненты систем искусственного интеллекта	*Шкала оценивания для зачета* *«Отлично»* (зачет) Показывает высокий уровень сформированности компетенций, т.е.: - демонстрирует высокое и прочное освоение материала; - исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал; - правильно формирует определения; - демонстрирует умения самостоятельной работы с нормативно-правовой литературой; - умеет делать выводы по излагаемому материалу. *«Хорошо» (зачет)* Показывает достаточный уровень сформированности компетенций, т.е.: - демонстрирует достаточно полное знание материала, основных теоретических положений; - достаточно последовательно, грамотно и логически стройно излагает теоретический материал; - демонстрирует умения ориентироваться в нормативно-правовой литературе; - умеет делать достаточно обоснованные выводы по излагаемому материалу. *«Удовлетворительно» (зачет)* Показывает пороговый уровень сформированности компетенций, т.е.: - демонстрирует общее знание изучаемого материала; - испытывает затруднения при ответах на дополнительные вопросы; - знает основную рекомендуемую литературу; - умеет строить ответ в соответствии со структурой излагаемого материала. *Неудовлетворительно» (незачет)* Ставится в случае: - незнания значительной части программного материала; - невладения понятийным аппаратом дисциплины; - допущения существенных ошибок при изложении учебного материала; - неумения строить ответ в соответствии со структурой излагаемого вопроса; - неумения делать выводы по излагаемому материалу.	Текущий контроль при проведении: - письменного/устного опроса; - тестирования; - оценки результатов самостоятельной работы (докладов, рефератов). Промежуточная аттестация в форме: -зачета, - письменных/ устных ответов, - тестирования.

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