

УТВЕРЖДАЮ
Проректор по учебной работе и
качеству образования

_____ И. А. Долгова

30 сентября 2026

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.02

Информационная безопасность

Направление подготовки:	45.04.04 Интеллектуальные системы в гуманитарной среде
Профиль подготовки:	Цифровая лингвистика
Квалификация:	магистр
Форма обучения:	очная
Год начала подготовки:	2027

Рабочая программа составлена в соответствии с:

- федеральным государственным образовательным стандартом высшего образования – магистратура по направлению подготовки 45.04.04 Интеллектуальные системы в гуманитарной среде, утверждённым приказом Министерства науки и высшего образования Российской Федерации от 13 августа 2020 года № 1003.

Разработчики программы: Юмашев В. Л., доцент; Кириллов А. Г., кандидат филологических наук, доцент

Рабочая программа согласована с руководителем образовательной программы 45.04.04 Интеллектуальные системы в гуманитарной среде. Рабочая программа рассмотрена и одобрена на заседании кафедры информационных систем и компьютерных технологий 10 сентября 2026, протокол № 2.

1. ОБЩАЯ ХАРАКТЕРИСТИКА

1.1. Цель и задачи дисциплины

Цель изучения дисциплины — формирование у обучающихся комплексной системы знаний, умений и практического опыта в области обеспечения информационной безопасности, защиты данных и верификации информации при решении профессиональных задач в сфере цифровой лингвистики

Задачи изучения дисциплины:

- формирование системы знаний о правовых, организационных и технологических основах информационной безопасности, методах защиты конфиденциальных данных и результатах интеллектуальной деятельности в цифровой среде;
- освоение методов критического анализа, верификации и оценки достоверности лингвистической информации, а также выявления деструктивного, манипулятивного контента и информационных угроз в сети Интернет;
- развитие умений определять релевантность и безопасность источников информации, соотносить разнородные риски уязвимости языковых данных и проектных ИТ-решений;
- овладение практическими навыками безопасного использования сетевых ресурсов, криптографической защиты данных, предотвращения несанкционированного доступа к разрабатываемому программному обеспечению и электронным языковым ресурсам.

1.2. Требования подготовленности обучающегося к освоению содержания дисциплины

Освоение дисциплины «Информационная безопасность» опирается на компетенции, сформированные у обучающихся в рамках предшествующего бакалаврского образования, а также в процессе освоения дисциплин 1–3 семестров магистратуры («Математика в гуманитарных науках», «Язык программирования Python», «Программирование в гуманитарной сфере», «Управление Интернет-контентом»).

Обучающийся перед началом освоения дисциплины должен:

Знать:

- основные принципы сбора, хранения и систематизации текстовой и цифровой информации;
- базовые стандарты форматирования электронных документов и структуры данных веб-страниц;
- синтаксис и принципы работы скриптов на языке программирования Python для автоматизации сбора информации (парсинга).

Уметь:

- работать в современных операционных системах на уровне уверенного пользователя и администратора локального ПК;
- осуществлять поиск, фильтрацию и структурирование данных в сети Интернет для решения научно-исследовательских задач;
- использовать веб-интерфейсы систем управления контентом (CMS) и репозитории контроля версий (Git/GitHub).

Владеть:

- навыками работы на персональном компьютере в сетевой среде;
- методами базовой компьютерной обработки текстовых массивов;
- инструментами первичного критического анализа научной и прикладной информации.

1.3. Планируемые результаты обучения по дисциплине

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	УК-1.1. Знает принципы сбора, систематизации и критического анализа информации	УК-1.1.1. Знает принципы сбора, систематизации и критического анализа информации с точки зрения её достоверности, конфиденциальности и защищенности в области цифровой лингвистики
	УК-1.2. Умеет определять релевантность источников информации, соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности	УК-1.2.1. Умеет определять релевантность и безопасность источников информации, соотносить разнородные угрозы безопасности лингвистических данных и систематизировать их в рамках профессиональной деятельности
	УК-1.3. Имеет практический опыт работы с информационными объектами и сетью Интернет	УК-1.3.1. Имеет практический опыт работы с информационными объектами и сетью Интернет с использованием инструментов криптографической защиты, проверки подлинности данных и безопасного поиска информации

2. ОБЪЁМ, СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объём дисциплины

Семестр	Контактная работа			СР	Форма ПА	Итоговый объём, часов/з. е.
	Л	П	ПА			
4	12	12	–	48	зачёт	72/2
Итого:	12	12	–	48		72/2

Л — лекции, П — все виды занятий семинарского типа, ПА — промежуточная аттестация, СР — самостоятельная работа обучающегося.

2.2. Структура дисциплины

Наименование тематического раздела дисциплины	Количество часов		
	Л	П	СР
Методологические основы информационной безопасности и верификации данных в цифровой среде	3	3	12
Правовые, организационные и лингвистические аспекты защиты данных и интеллектуальной собственности	3	3	12
Технологические и криптографические средства лингвобезопасности	3	3	12
Безопасность сетевых коммуникаций и критический анализ медиаконтента	3	3	12
Всего:	12	12	48

2.3. Содержание тематических разделов дисциплины

Раздел 1. Методологические основы информационной безопасности и верификации данных в цифровой среде
Понятие информационной безопасности и лингвобезопасности. Субъекты информационных отношений в сетевом пространстве. Категории и типы уязвимости текстовой и языковой информации. Основные виды информационных угроз и атак на данные. Феномен информационного шума. Методология критического анализа и верификации сетевой информации на основе принципов достоверности, полноты и конфиденциальности. Направления и стратегии комплексной защиты профессиональной информации лингвиста.
Раздел 2. Правовые, организационные и лингвистические аспекты защиты данных и интеллектуальной собственности
Законодательство Российской Федерации в области защиты информации и персональных данных применительно к веб-ресурсам и сетевой коммуникации. Правовая и техническая защита объектов интеллектуальной собственности в цифровой лингвистике: защита авторских прав на разработанное программное обеспечение (скрипты, парсеры), собранные языковые корпуса и базы данных. Моделирование угроз несанкционированного доступа к профессиональным ресурсам. Международные и отечественные стандарты организационной защиты информации. Разграничение прав доступа в системах управления контентом (CMS).

Раздел 3. Технологические и криптографические средства лингвобезопасности
--

Комплексная защита автоматизированных систем обработки текстовой информации. Современные криптографические методы защиты данных: симметричное и асимметричное шифрование, электронная цифровая подпись, SSL/TLS-протоколы защиты веб-трафика. Вредоносный программный код, уязвимости веб-скриптов и методы их нейтрализации. Технологические средства защиты коммерческой и академической информации. Инструменты контроля версий (Git/GitHub) как элемент обеспечения целостности и защищенности программного кода.
--

Раздел 4. Безопасность сетевых коммуникаций и критический анализ медиаконтента

Особенности распространения и защиты информации в распределенных телекоммуникационных сетях. Уязвимости протоколов передачи лингвистических данных. Информационные угрозы в медиасреде и социальных сетях: лингвистические маркеры речевой манипуляции, деструктивного контента, фейковых новостей (fake news) и диффамации. Методы автоматизированного мониторинга, контент-анализа и выявления угроз информационной гигиены в сети Интернет. Обеспечение безопасности сетевой инфраструктуры лингвистических ИТ-проектов.
--

2.4. Организация учебных занятий

Дисциплина может реализовываться с применением электронного обучения и дистанционных образовательных технологий.

3. ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

3.1. Учебная литература

3.1.1. Основная

1. Вострецова, Е. В. Основы информационной безопасности : учебное пособие / Е. В. Вострецова ; Уральский федеральный университет им. первого Президента России Б. Н. Ельцина. – Екатеринбург : Издательство Уральского университета, 2019. – 207 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=697636>.
2. Технологии обеспечения безопасности информационных систем : учебное пособие : [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. : ил., схем., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=598988>.

3.1.2. Дополнительная

1. Брюхомицкий, Ю. А. Безопасность информационных технологий : учебное пособие : в 2 частях : [16+] / Ю. А. Брюхомицкий ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2020. – Часть 1. – 171 с. : ил., табл., схем., граф. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=612167>.
2. Информационная безопасность в цифровом обществе : учебное пособие : [16+] / А. С. Исмагилова, И. В. Салов, И. А. Шагапов, А. А. Корнилова ; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2019. – 128 с. : табл., ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=611084>.
3. Литвиненко, О. В. Правовые аспекты информационной безопасности : учебное пособие : [16+] / О. В. Литвиненко. – Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2021. – 63 с. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=694774>.
4. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие : [16+] / А. В. Моргунов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=576726>.

3.2. Профессиональные базы данных и информационные справочные системы

Наименование ресурса	Адрес	Тип доступа
Электронно-библиотечные системы		
ЭБС «Университетская библиотека онлайн»	https://biblioclub.ru/	Индивидуальный неограниченный доступ после регистрации
КиберЛенинка, российская научная электронная библиотека	https://cyberleninka.ru/	Открытый ресурс

Наименование ресурса	Адрес	Тип доступа
Профессиональные базы данных и информационные справочные системы		
eLIBRARY.RU, российский информационно-аналитический портал	https://elibrary.ru/	Открытый ресурс
Банк данных угроз безопасности информации ФСТЭК	https://bdu.fstec.ru/	Открытый ресурс
Справочно-правовая система «Консультант Плюс»	https://www.consultant.ru/	Открытый ресурс; по подписке

3.3. Сетевые ресурсы

Наименование ресурса	Адрес
Information Security Stack Exchange	https://security.stackexchange.com/

3.4. Методическое обеспечение дисциплины

3.4.1. Методические указания для преподавателя

Изучение дисциплины проводится в форме лекций, практических занятий, организации самостоятельной работы студентов, консультаций.

Лекции реализуются через изложение учебного материала с возможным мультимедийным сопровождением. Основными целями лекции являются системное освещение ключевых понятий и положений по соответствующей теме, обзор и оценка существующей проблематики, её методологических и социокультурных оснований, возможных вариантов решения, предложение методических рекомендаций для дальнейшего изучения курса, в том числе литературы и источников. Лектор должен стимулировать обучающихся к участию в обсуждении вопросов лекционного занятия, к высказыванию собственной точки зрения по обсуждаемой проблеме. Главное назначение лекции — обеспечить теоретическую основу обучения, развить интерес к учебной деятельности и конкретной учебной дисциплине, сформировать у обучающихся ориентиры для самостоятельной работы над курсом.

Практические занятия направлены на развитие самостоятельности обучающихся в исследовании изучаемых вопросов и приобретение умений и навыков. Практические занятия традиционно проводятся в форме обсуждения проблемных вопросов в группе при активном участии обучающихся. Они способствуют углубленному изучению наиболее фундаментальных и сложных проблем курса, служат важной формой анализа и синтеза исследуемого материала, а также подведения итогов самостоятельной работы обучающихся, стимулируя развитие профессиональной компетентности, навыков и умений. На практических занятиях обучающиеся учатся работать с научной литературой, чётко и доходчиво излагать проблемы и предлагать варианты их решения, аргументировать свою позицию, оценивать и критиковать позиции других, свободно публично высказывать свои мысли и суждения, грамотно вести полемику и представлять результаты собственных исследований. Практические занятия проводятся в форме устных и письменных опросов, диспута, тестирования, выполнения заданий, обсуждения докладов, выполнения контрольных заданий и пр.

Результаты работы на практических занятиях учитываются преподавателем при выставлении итоговой оценки по данной дисциплине. На усмотрение преподавателя обучающиеся, активно отвечающие на занятиях и выполняющие рекомендации преподавателя

при подготовке к ним, могут получить повышающий балл к своей оценке в рамках промежуточной аттестации.

3.4.2. Методические рекомендации по самостоятельной работе обучающихся

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых во время аудиторной работы. Во время самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Самостоятельная работа включается в общую трудоёмкость учебной нагрузки обучающегося.

Реализация поставленной цели предполагает решение следующих задач:

- освоение и расширение теоретических знаний по изучаемой дисциплине;
- систематизация и закрепление полученных теоретических знаний и практических навыков;
- формирование умений по поиску и использованию нормативной, справочной и специальной литературы, а также других источников информации;
- развитие познавательных способностей и активности, творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самообразованию, самосовершенствованию и самореализации;
- развитие научно-исследовательских навыков;
- формирование умения решать практические задачи (в профессиональной деятельности), используя приобретённые знания, способности и навыки.

Самостоятельная работа должна быть выполнена индивидуально или являться частью коллективной работы (в случае выполнения группового задания в работе делается соответствующая оговорка).

3.5. Материально-техническое обеспечение дисциплины

3.5.1. Аудитории для проведения занятий

Специальные помещения представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, выполнения курсовых работ, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования.

Специальные помещения укомплектованы учебной мебелью, в том числе мебелью для преподавателя дисциплины, учебной доской.

Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечиваются электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Материально-техническое оснащение учебных аудиторий конкретизировано на официальном сайте Университета в подразделе «Материально-техническое обеспечение и оснащённость образовательного процесса. Доступная среда» раздела «Сведения об образовательной организации».

3.5.2. Оборудование и технические средства обучения

Специальные помещения укомплектованы демонстрационным оборудованием (мультимедийный проектор, экран, компьютер, звуковые колонки).

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду Университета.

Электронно-библиотечная система (электронная библиотека) и электронная информационно-образовательная среда обеспечивают одновременный доступ не менее 25 процентов обучающихся.

3.5.3. Программное обеспечение

Наименование	Сведения о лицензии
Moodle, среда дистанционного обучения	GNU GPL, свободно распространяемое с открытым исходным кодом
GnuPG	GNU GPL, свободно распространяемое с открытым исходным кодом
VeraCrypt	GNU GPL, свободно распространяемое с открытым исходным кодом
КриптоПро CSP	Проприетарное программное обеспечение

4. ОЦЕНОЧНЫЕ СРЕДСТВА

4.1. Методика проведения текущего контроля успеваемости и промежуточной аттестации

Оценивание уровня учебных достижений обучающихся по дисциплине осуществляется в виде текущего контроля успеваемости и промежуточной аттестации. Фонд оценочных средств по дисциплине включает оценочные материалы, направленные на проверку освоения компетенций, в том числе знаний, умений и навыков. Фонд оценочных средств включает оценочные средства текущего контроля и оценочные средства промежуточной аттестации.

4.1.1. Балльно-рейтинговая карта дисциплины

Виды работы	Виды контроля, критерии оценки и количество баллов
Текущий контроль	
Аудиторная работа (0-20 баллов)	Посещение занятий и участие в работе: 10 баллов — посещение не менее 50% занятий 15 баллов — посещение 60-80% занятий, участие в обсуждениях материала 20 баллов — посещение 90-100% занятий, активное участие в обсуждениях материала
Самостоятельная работа (0-40 баллов)	Выполнение тестов и практических работ в СДО Moodle
Промежуточная аттестация	
Контрольное задание (0-40 баллов)	Выполнение письменного контрольного задания в СДО Moodle

4.1.2. Шкала перевода рейтинговых баллов в пятибалльную систему оценивания

Общее количество баллов	Оценка сформированности компетенций	Оценка результатов обучения по дисциплине	Оценка ECTS
0–34	Компетенции не сформированы.	неудовлетворительно (не зачтено)	F
Теоретическое содержание не освоено, практические навыки не сформированы, большинство учебных заданий не выполнено, качество их выполнения минимальное, все задания содержат грубые ошибки. Обучающийся не готов решать типовые профессиональные задачи.			
35–49	Уровень владения компетенциями недостаточный для их формирования в результате обучения по дисциплине.	неудовлетворительно (не зачтено)	FX
Теоретическое содержание освоено частично, практические навыки не сформированы, большинство учебных заданий не выполнено, качество их выполнения минимальное, большинство заданий выполнено с ошибками. Обучающийся не готов решать типовые профессиональные задачи.			
50–59	Уровень владения компетенциями	удовлетворительно	E

Общее количество баллов	Оценка сформированности компетенций	Оценка результатов обучения по дисциплине	Оценка ECTS
	посредственный для их формирования в результате обучения по дисциплине.	(зачтено)	
Теоретическое содержание освоено частично, практические навыки сформированы фрагментарно, многие учебные задания не выполнены, качество их выполнения минимальное, многие задания выполнены с ошибками. Обучающийся готов решать типовые профессиональные задачи.			
60–69	Уровень владения компетенциями удовлетворительный для их формирования в результате обучения по дисциплине.	удовлетворительно (зачтено)	D
Теоретическое содержание освоено частично, пробелы не носят существенного характера, практические навыки в основном сформированы, большинство учебных заданий выполнено, качество их выполнения удовлетворительное, некоторые задания выполнены с ошибками. Обучающийся готов решать типовые профессиональные задачи.			
70–89	Уровень владения компетенциями преимущественно высокий для их формирования в результате обучения по дисциплине.	хорошо (зачтено)	C
Теоретическое содержание освоено полностью, некоторые практические навыки сформированы недостаточно, все учебные задания выполнены, качество их выполнения высокое, некоторые задания выполнены с ошибками. Обучающийся готов решать типовые и ситуативные профессиональные задачи.			
90–94	Уровень владения компетенциями высокий для их формирования в результате обучения по дисциплине.	отлично (зачтено)	B
Теоретическое содержание освоено полностью, практические навыки сформированы, все учебные задания выполнены, качество их выполнения близко к максимальному, однако есть несколько незначительных ошибок. Обучающийся готов эффективно решать типовые и ситуативные профессиональные задачи, в том числе повышенного уровня сложности.			
95–100	Уровень владения компетенциями превосходный для их формирования в результате обучения по дисциплине.	отлично (зачтено)	A
Теоретическое содержание освоено полностью, практические навыки сформированы, все учебные задания выполнены, качество их выполнения близко к максимальному. Обучающийся готов эффективно решать типовые и ситуативные профессиональные задачи, в том числе повышенного уровня сложности, и способен разрабатывать новые решения.			

4.2. Оценочные средства текущего контроля

4.2.1. Вопросы для подготовки к семинарским занятиям

Раздел 1. Методологические основы информационной безопасности и верификации данных в цифровой среде

1. Дайте определения базовым понятиям ИБ: конфиденциальность, целостность, доступность, аутентичность, апеллируемость применительно к электронным текстовым ресурсам.
2. Что понимается под терминами «информационная безопасность» и «лингвобезопасность» в сетевом пространстве? В чем их пересечение и различия?
3. Перечислите основных субъектов информационных отношений в Интернете и опишите специфику их уязвимости.
4. Какие существуют разновидности и типы угроз текстовой и языковой информации?
5. Какие действия злоумышленников приводят к неправомерному овладению профессиональной информацией лингвиста (базами данных, словарями)?
6. Дайте характеристику феномену информационного шума: причины возникновения, влияние на качество лингвистических данных и методы минимизации.
7. Раскройте содержание понятий «достоверность», «полнота» и «конфиденциальность» как основы методологии верификации сетевого контента.
8. Какие существуют общеметодологические направления и стратегии обеспечения информационной безопасности лингвистических ИТ-проектов?
9. Опишите виды и психологические механизмы социальной инженерии в контексте несанкционированного доступа к текстовой информации.
10. Какие существуют современные методы критического анализа и верификации текстовых данных, полученных из открытых интернет-источников?
11. Каковы особенности защиты приватности и персональных данных пользователей при фиксации их речевого поведения в телекоммуникационных сетях?
12. Каким образом принципы информационной гигиены влияют на методологию формирования репрезентативных лингвистических выборок?

Раздел 2. Правовые, организационные и лингвистические аспекты защиты данных и интеллектуальной собственности

1. Назовите основные законодательные акты Российской Федерации в области защиты информации и персональных данных.
2. Каковы особенности правовой обработки персональных данных при проектировании веб-ресурсов, форумов и систем сетевой коммуникации?
3. Что такое модель угроз информации предприятия/ИТ-проекта и как она строится в цифровой гуманитаристике?
4. Опишите специфику правовой и технической защиты авторских прав на разработанное лингвистическое ПО (скрипты, парсеры, модули NLP).
5. Каковы правовые основания и особенности защиты интеллектуальной собственности при формировании, разметке и публикации больших языковых корпусов и баз данных?
6. Разработайте концептуальную модель угроз несанкционированного доступа к закрытому профессиональному лингвистическому ресурсу (например, платному электронному словарю).
7. Охарактеризуйте международные и отечественные стандарты (ISO, ГОСТ) организационной и административной защиты корпоративной информации.
8. Какие существуют модели управления доступом к информации и как они реализуются на практике?
9. Опишите принципы разграничения прав доступа и настройки ролевых моделей пользователей в современных системах управления контентом (CMS).
10. С какими юридическими рисками сталкивается лингвист при автоматизированном сборе (парсинге) открытых текстовых массивов в сети Интернет?
11. В чем заключаются особенности защиты интеллектуальной собственности и авторского права в условиях построения единого пространства сети Интернет?
12. Каковы меры административной и правовой ответственности за утечку конфиденциальных лингвистических данных и коммерческих глоссариев?

Раздел 3. Технологические и криптографические средства лингвобезопасности

1. Каковы особенности инженерно-технического и программно-аппаратного направлений защиты автоматизированных систем обработки текстов?
2. Опишите принцип работы, достоинства и недостатки алгоритмов симметричного шифрования при передаче текстовых файлов.
3. Опишите принцип работы асимметричного шифрования (с открытым ключом). В чем его преимущество для защиты сетевого обмена?
4. Для чего применяется электронная цифровая подпись (ЭЦП) и каков математический и технологический принцип ее функционирования?
5. Как работают криптографические протоколы защиты веб-трафика SSL/TLS и какую роль в этой системе играет сертификат сайта?
6. Какие существуют виды вредоносных программ и каковы основные каналы их внедрения в автоматизированные лингвистические процессоры?
7. Какие уязвимости веб-скриптов и программные угрозы (кроме вредоносного ПО) представляют опасность для интерактивных языковых сервисов?
8. Классифицируйте виды злоумышленников (хакеров) в электронной среде по уровню их квалификации и потенциальным мотивам.
9. Опишите современные функции, эвристические и сигнатурные методы работы антивирусных средств защиты.
10. Как работают средства резервного копирования (бэкапа) данных и каковы стратегии их применения для обеспечения целостности баз языковых данных?
11. Каким образом инструменты контроля версий (Git/GitHub) выступают в качестве элемента обеспечения целостности и защищенности исходного программного кода?
12. Опишите технические и криптографические средства защиты коммерческой и академической текстовой информации от утечек (DLP-системы).

Раздел 4. Безопасность сетевых коммуникаций и критический анализ медиаконтента

1. Опишите ключевые особенности, уязвимости и проблемы распространения информации в распределенных телекоммуникационных сетях.
2. В чем заключаются уязвимости современных сетевых протоколов при передаче и синхронизации распределенных лингвистических данных?
3. Охарактеризуйте основные уязвимости и особенности защиты текстовой информации в каналах электронной почты и современных мессенджерах.
4. Назовите и опишите лингвистические маркеры и приемы скрытой речевой манипуляции в медиасреде и социальных сетях.
5. Что такое деструктивный контент в Интернете с точки зрения лингвистической экспертизы и каковы методы его автоматического обнаружения?
6. Каковы языковые и структурные маркеры фейковых новостей (fake news)? На основе каких критериев алгоритмы ИИ осуществляют их первичную фильтрацию?
7. Что такое диффамация и речевая агрессия в цифровом дискурсе, и каковы современные методы их лингвистического и автоматизированного анализа?
8. Какие существуют программные инструменты для автоматизированного мониторинга и контент-анализа медиaprостранства в целях выявления угроз ИБ?
9. Каким образом обеспечивается базовая защита сетевой инфраструктуры и серверов, на которых развернуты лингвистические ИТ-проекты (брандмауэры, прокси)?
10. Какие существуют средства и программные решения для сетевой защиты оконечных устройств (ПК, смартфонов) пользователей?
11. Охарактеризуйте принципы организации «информационной гигиены» для специалистов, работающих с большими потоками немодерируемого интернет-контента.
12. Как установить полезные профессиональные контакты в сфере кибербезопасности и лингвоэкспертизы на научных мероприятиях, и как оценивать уровень их организации?

Критерии оценки работы на практическом занятии

Критерии	Максимальное количество
----------	-------------------------

	баллов за занятие
Устный опрос, коллоквиум	
Основные теоретические положения по вопросу раскрыты. Имеются элементы обоснования выводов. Имеются элементы систематизации информации, факты применения профессиональной терминологии. Очевидно использование источников рекомендованной литературы.	5 баллов

4.2.2. Темы докладов

1. Современное законодательство РФ в области защиты информации и особенности его применения к текстовому контенту веб-ресурсов.
2. Правовая и техническая защита объектов интеллектуальной собственности в цифровой лингвистике: регистрация прав на языковые корпуса, базы данных и авторские скрипты.
3. Особенности обработки персональных данных при автоматизированном сборе (парсинге) открытых интернет-пространств и формировании лингвистических выборок.
4. Разработка и пример построения модели угроз несанкционированного доступа для электронной библиотечной системы или интерактивного языкового сервиса.
5. Влияние развития квантовых вычислений на современную криптографию и защиту распределенных баз данных.
6. Влияние развития генеративного искусственного интеллекта (LLM) на отрасль защиты информации и кибербезопасность.
7. Проблемы защиты авторских прав и интеллектуальной собственности на тексты в эпоху обучения больших языковых моделей (LLM).
8. Глобальные разведывательные альянсы (Альянс «Пять глаз» и аналоги) и их влияние на стандарты приватности в сети Интернет.
9. Технологии разграничения прав доступа и обеспечения безопасности контента в современных CMS (системах управления контентом).
10. Современные криптографические протоколы (SSL/TLS) и средства защиты веб-трафика интерактивных лингвистических ИТ-проектов.
11. Инструменты контроля версий (Git/GitHub) как элемент технологического контроля целостности и защищенности исходного программного кода.
12. Проблема приватности пользователей в сети Интернет: методы деанонимизации на основе стилометрического и автороведческого анализа текста.
13. Архитектура сквозного шифрования (End-to-End) и средства защиты текстовых данных в современных мессенджерах.
14. Законодательные инициативы государств по усилению контроля за медиаконтентом и соблюдением информационной гигиены в сети Интернет.
15. Лингвистические маркеры и приемы речевой манипуляции в деструктивном сетевом контенте: методы автоматического обнаружения.
16. Технологии распознавания фейковых новостей (fake news) на основе автоматизированного контент-анализа и NLP-пайплайнов.
17. Лингвистическая экспертиза диффамации и речевой агрессии в цифровом дискурсе социальных сетей.
18. Использование методов социальной инженерии в сети Интернет: лингвистический анализ фишинговых текстов и сценариев мошенничества.

Шкала и критерии оценки доклада

Критерии	Показатели	Баллы
1. Степень раскрытия сущности проблемы	– соответствие теме доклада; – полнота и глубина раскрытия основных понятий; – умение работать с литературой, систематизировать и структурировать материал; – умение обобщать, сопоставлять различные точки зрения по рассматриваемому вопросу, аргументировать основные положения и выводы.	70
2. Обоснованность выбора источников	– круг, полнота использования литературных источников по теме; – привлечение новейших работ (журнальные публикации, материалы сборников научных трудов и т.д.).	15
3. Изложение	– литературный стиль.	15

Доклад оценивается по 100 балльной шкале, баллы переводятся в оценки успеваемости следующим образом:

90 – 100 баллов – «отлично»;

70 – 89 баллов – «хорошо»;

50 – 69 баллов – «удовлетворительно»;

менее 50 баллов – «неудовлетворительно».

4.3. Оценочные средства промежуточной аттестации

4.3.1. Контрольные задания

Прочитайте текст и установите соответствие.

Установите соответствие между задачей по защите информации и типом защитного программного обеспечения:

А. Защита от вредоносных программ Б. Защита от сетевых атак извне В. Защита от утечек данных из организации Г. Защита конфиденциальности на сменных носителях Д. Обмен зашифрованной электронной почтой	1. DLP 2. Антивирус 3. ПО для шифрования 4. Сертификаты 5. МСЭ
---	--

Запишите выбранные цифры под соответствующими буквами:

А	Б	В	Г	Д

Прочитайте текст и установите последовательность.

Расположите методы шифрования в порядке их появления (исторически) от самого старого до самого нового:

А. Постквантовая криптография

Б. Симметричная криптография

В. Криптография с открытым ключом

Запишите соответствующую последовательность букв:

--

Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа.

Кто должен создавать ключи в алгоритмах с открытым ключом?

- А. отправитель сообщений
- Б. получатель сообщений
- В. удостоверяющий центр

Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа.

Как называется тип атаки, когда противник может вставлять, удалять или повторять сообщения, вклиниваясь между переговаривающимися партнерами?

- А. пассивная атака
- Б. нейтральная атака
- В. активная атака

Прочитайте текст и установите соответствие.

Установите соответствие между категорией информации и ее определением:

А. Конфиденциальность Б. Аутентичность В. Неотказуемость Г. Доступность	1. Способность удостоверить имевшее место действие или событие так, чтобы эти события или действия не могли быть позже отвергнуты. 2. Свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса. 3. Свойство объекта находиться в состоянии готовности и используемости по запросу авторизованного логического объекта. 4. Свойство, гарантирующее, что источником информации является именно то лицо, которое заявлено как её автор.
--	--

Запишите выбранные цифры под соответствующими буквами:

А	Б	В	Г

Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов.

Выберите из приведенного три направления защиты информации:

- А. инженерно-техническое
- Б. социальное
- В. правовое
- Г. экономическое
- Д. организационное
- Е. общественно-политическое

Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов.

Какие из приведенных функций – функции антивирусов?

- А. препятствование проникновению вирусов в компьютерную систему
- Б. обнаружение наличия вирусов в компьютерной системе
- В. защита от нежелательной рекламы
- Г. устранение вирусов из компьютерной системы
- Д. защита от фишинговых атак

Прочитайте текст и запишите развёрнутый обоснованный ответ.

Что такое хэш функция, для чего применяется?

--

Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов.

Какие параметры из приведенных обязательно присутствуют в любом сертификате X.509?

- А. имя сайта
- Б. открытый ключ субъекта
- В. срок действия сертификата
- Г. адрес электронной почты
- Д. название организации, заказавшей сертификат
- Е. серийный номер сертификата

Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа.

Какое утверждение верно по отношению к компьютерным вирусам?

- А. заражают любые файлы, содержащие исполняемые инструкции
- Б. заражают только исполняемые файлы
- В. заражают только файлы документов с макросами
- Г. заражают только почтовые вложения

Прочитайте текст и запишите развёрнутый обоснованный ответ.

Нарисуйте схему работы шифрования с открытым ключом, указав этапы: создание ключей, процесс шифрования, процесс расшифровывания.

--

Прочитайте текст и запишите развёрнутый обоснованный ответ.

Нарисуйте схему подписывания с использованием открытого и закрытого ключа:

--

Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов.

Какие из приведенных элементов, входят в концептуальную модель безопасности?

- А. угрозы
- Б. выпускаемая продукция
- В. услуги других организаций
- Г. источники информации
- Д. способы защиты информации

Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов.

Какие два типа доступа существуют с точки зрения модели безопасности?

- А. чтение
- Б. создание
- В. запись
- Г. удаление

Прочитайте текст и запишите развёрнутый обоснованный ответ.

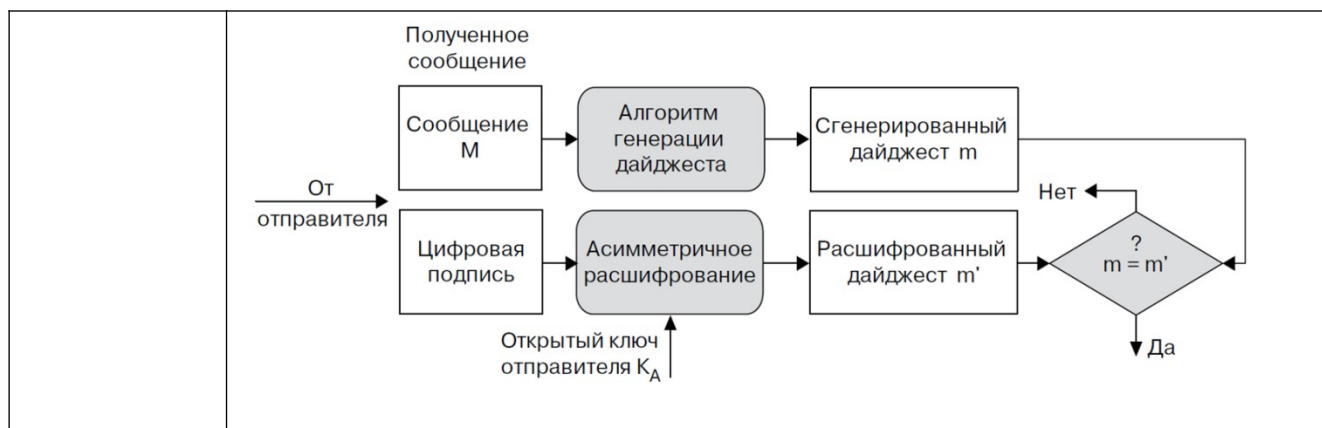
Нарисуйте схему подписывания и проверки подписи в современных системах, где подписывается не все сообщение а его дайджест:

--

4.3.2. Ключи к контрольным заданиям

	A2B5B1ГЗД4
	231
	Б В шифровании с открытым ключом тот, кто хочет получать зашифрованные сообщения, должен создать пару ключей – открытый и закрытый. Закрытый ключ хранится у него, а открытый выкладывается в публичный доступ.
	В В случае пассивной атаки атакующий только прослушивает коммуникации, но не может на них влиять. Понятия «нейтральная» атака не существует.
	A2B4B1ДЗ
	АБГ Существует только три направления защиты информации. Остальные указанные пункты не относятся к направлениям защиты.
	АБГ Защита от нежелательной рекламы не является функцией антивируса, хотя может быть включено разработчиком в комплексный много функциональный программный продукт. Защита от фишинговых атак также не является функцией антивируса, хотя и добавляется в функционал некоторыми производителями.
	Хэш функция – это алгоритм, преобразующий входные данные любого объема (файл, текст) в уникальную строку фиксированной длины (хэш-сумма). Она работает необратимо: по хэшу нельзя восстановить данные. Одинаковый вход всегда дает один хэш, а малейшее изменение данных меняет хэш до неузнаваемости. Используется для проверки целостности данных, хранения паролей и в блокчейне.
	БВЕ Из приведенного списка в любом сертификате будет присутствовать открытый ключ субъекта, срок действия сертификата с определенной даты по определенную дату, серийный номер сертификата. Адрес электронной почты могут быть в персональных сертификатах для электронной почты. Адрес сайта указывается только в сертификатах сайтов. Название организации используется только в небольшом числе узкоспециализированных сертификатов.
	А Заражаться могут любые файлы, которые содержат инструкции для исполнения либо программного кода, либо инструкции для интерпретации некоторого кода, например, макросы или скрипты в документах.

	Открытый ключ используется для зашифрования Сервер открытых ключей Закрытый ключ используется для расшифрования Публикация открытого ключа Закрытый Открытый Получатель должен создать два связанных ключа
	Подпись верна или не верна Проверка ЭП Создание ЭП Открытый ключ используется для проверки ЭЦП Сервер открытых ключей Закрытый ключ используется для создания ЭЦП Публикация открытого ключа Закрытый Открытый Получатель должен создать два связанных ключа
	АГД Выпускаемая продукция не является ни объектом, ни субъектом обработки информации. Услуги других организаций не входят в модель, а только могут влиять на состав угроз и источников информации.
	АВ Создание и удаление являются частным случаем доступа на запись.
	Создание подписи Сообщение M Алгоритм генерации дайджеста Дайджест m сообщения Асимметричное шифрование Секретный ключ отправителя k_A Цифровая подпись Отправляемое сообщение Сообщение M К получателю Проверка подписи



Шкала и критерии оценки текущего тестирования

Число правильных ответов	Оценка
90-100% правильных ответов	Оценка «отлично»
70-89% правильных ответов	Оценка «хорошо»
50-69% правильных ответов	Оценка «удовлетворительно»
Менее 50% правильных ответов	Оценка «неудовлетворительно»

5. ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ В ОТНОШЕНИИ ЛИЦ ИЗ ЧИСЛА ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Профессорско-преподавательский состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Министерства науки и высшего образования Российской Федерации, в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создания комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учётом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Согласно требованиям к порядку реализации образовательной деятельности в отношении инвалидов и лиц с ОВЗ, установленным Министерством науки и высшего образования Российской Федерации, необходимо иметь в виду, что:

1) инвалиды и лица с ОВЗ по зрению имеют право присутствовать на занятиях вместе с ассистентом, оказывающим обучающемуся необходимую помощь;

2) инвалиды и лица с ОВЗ по слуху имеют право на использование звукоусиливающей аппаратуры.

При проведении промежуточной аттестации по дисциплине обеспечивается соблюдение следующих общих требований:

- проведение аттестации для инвалидов в одной аудитории совместно с обучающимися, не являющимися инвалидами, если это не создает трудностей для инвалидов и иных обучающихся при промежуточной аттестации;

- присутствие в аудитории ассистента (ассистентов), оказывающего обучающимся инвалидам необходимую техническую помощь с учётом их индивидуальных особенностей (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с экзаменатором);

- пользование необходимыми обучающимся инвалидам техническими средствами при прохождении промежуточной аттестации с учётом их индивидуальных особенностей;

- обеспечение возможности беспрепятственного доступа обучающихся инвалидов в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях.

По письменному заявлению обучающегося инвалида продолжительность прохождения испытания промежуточной аттестации (зачёта, экзамена, и др.) обучающимся инвалидом может быть увеличена по отношению к установленной продолжительности его сдачи:

- продолжительность сдачи испытания, проводимого в письменной форме, — не более чем на 90 минут;

- продолжительность подготовки обучающегося к ответу, проводимому в устной форме, — не более чем на 20 минут.

В зависимости от индивидуальных особенностей обучающихся с ОВЗ Университет обеспечивает выполнение следующих требований при проведении аттестации:

а) для слепых:

- задания и иные материалы для прохождения промежуточной аттестации оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, либо зачитываются ассистентом;

- письменные задания выполняются обучающимися на бумаге рельефно-точечным шрифтом Брайля или на компьютере со специализированным программным обеспечением для слепых, либо надиктовываются ассистенту;

- при необходимости обучающимся предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным обеспечением для слепых;

б) для слабовидящих:

- задания и иные материалы для сдачи экзамена оформляются увеличенным шрифтом;

- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

- при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

в) для глухих и слабослышащих, с тяжелыми нарушениями речи:

- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающимся предоставляется звукоусиливающая аппаратура индивидуального пользования;

- по их желанию испытания проводятся в письменной форме;

г) для лиц с нарушениями опорно-двигательного аппарата (тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

- письменные задания выполняются обучающимися на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;

- по их желанию испытания проводятся в устной форме.

О необходимости обеспечения специальных условий для проведения аттестации обучающийся должен сообщить письменно не позднее, чем за 10 дней до начала аттестации. К заявлению прилагаются документы, подтверждающие наличие у обучающегося индивидуальных особенностей (при отсутствии указанных документов в организации).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.