

УТВЕРЖДАЮ
Проректор по учебной работе и
качеству образования

_____ И. А. Долгова

15 апреля 2026

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.25

Информационная безопасность

Направление подготовки:	45.03.04 Интеллектуальные системы в гуманитарной сфере
Профиль подготовки:	Цифровая лингвистика
Квалификация:	бакалавр
Форма обучения:	очная
Год начала подготовки:	2026

Рабочая программа составлена в соответствии с:

- федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению подготовки 45.03.04 Интеллектуальные системы в гуманитарной сфере, утверждённым приказом Министерства образования и науки Российской Федерации от 24 апреля 2018 года № 324.

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

Рабочая программа согласована с руководителем образовательной программы 45.03.04 Интеллектуальные системы в гуманитарной сфере. Рабочая программа рассмотрена и одобрена на заседании кафедры информационных систем и компьютерных технологий 27 февраля 2026, протокол № 7.

1. ОБЩАЯ ХАРАКТЕРИСТИКА

1.1. Цель и задачи дисциплины

Цель изучения дисциплины — изучение основных принципов, методов и средств защиты информации в процессе её обработки, передачи и хранения с использованием компьютерных средств в информационных системах. формирование у обучающихся системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации.

Задачи изучения дисциплины:

- формирование знаний о концепциях защиты информации и системах безопасности персональных компьютеров и компьютерных сетей, организационно-правовом обеспечении информационной безопасности;
- формирование знаний об основных методах и приёмах защиты информации;
- овладение способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности;
- формирование навыков обеспечения защиты объектов интеллектуальной собственности, результатов исследований и разработок.

1.2. Требования подготовленности обучающегося к освоению содержания дисциплины

Обучающийся по дисциплине «Информационная безопасность» должен иметь знания, умения и навыки, полученные при практическом использовании информационных технологий в учебной и научной деятельности. Обучающийся должен уметь использовать средства для работы с ресурсами сети Интернет (веб-браузеры), иметь навыки работы с офисными пакетами, подготовки документов.

1.3. Планируемые результаты обучения по дисциплине

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
ОПК-5. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-5.2. Использует современные информационные технологии в профессиональной деятельности	ОПК-5.2.1. Знает содержание, структуру и принципы работы современных информационных технологий, применяемых для решения задач профессиональной деятельности
		ОПК-5.2.2. Умеет обоснованно выбирать современные информационные технологии, компьютерное и сетевое оборудование, программное обеспечение для решения задач профессиональной деятельности

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
		ОПК-5.2.3. Владеет навыками применения современных информационных технологий и программного обеспечения при решении задач профессиональной деятельности

2. ОБЪЁМ, СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объём дисциплины

Семестр	Контактная работа			СР	Форма ПА	Итоговый объём, часов/з. е.
	Л	П	ПА			
6	16	16	–	40	зачёт	72/2
Итого:	16	16	–	40		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
Основы информационной безопасности	2	2	4
Правовые и административные средства защиты информации	2	2	6
Техническая защита информации	8	8	20
Защита информации в телекоммуникационных сетях	4	4	10
Всего:	16	16	40

2.3. Содержание тематических разделов дисциплины

Раздел 1. Основы информационной безопасности
Термины и определения. Субъекты информационных отношений. Категории информации. Методы обеспечения информационной безопасности и защиты информации. Угрозы информации. Атаки на информацию. Действия, приводящие к неправомерному овладению информацией. Направления защиты информации.
Раздел 2. Правовые и административные средства защиты информации
Законодательство в области защиты информации. Персональные данные и их обработка. Интеллектуальная собственность и её защита. Модели угроз. Организационное направление защиты. Модели доступа.
Раздел 3. Техническая защита информации
Комплексная защита информационных систем. Инженерно-технические средства защиты. Современные средства криптографии. Злоумышленники и вредоносные программы, способы и средства защиты от них. Технические средства защиты интеллектуальной собственности.
Раздел 4. Защита информации в телекоммуникационных сетях
Особенности распространения информации в телекоммуникационных сетях. Особенности угроз информации в сетях. Средства защиты информации в сетях предприятий и организаций. Особенности построения сети Интернет и особенности защиты информации в ней.

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. Основы информационной безопасности

1. Дайте определения понятиям: конфиденциальность, целостность, доступность, аутентичность, апеллируемость.

2. Какие существуют методы обеспечения информационной безопасности и защиты информации?
3. Какие существуют разновидности угроз информации?
4. Какие существуют действия, приводящие к неправомерному овладению информацией?
5. Опишите направления обеспечения информационной безопасности и защиты информации.

Раздел 2. Правовые и административные средства защиты информации

1. Назовите основные законодательные акты в области защиты информации.
2. Что такое персональные данные и какие есть особенности их обработки?
3. Что такое модель угроз информации предприятия?
4. Как строится модель угроз?
5. Какие существуют модели доступа к информации?

Раздел 3. Техническая защита информации

1. Опишите разделы инженерно-технического направления защиты информации.
2. Опишите принцип работы симметричного шифрования.
3. Опишите принцип работы шифрования с открытым ключом.
4. Опишите принцип работы электронной подписи, для чего применяется.
5. Какие существуют виды вредоносных программ?
6. Какие существуют программные угрозы помимо вредоносных программ?
7. Какие существуют виды злоумышленников?
8. Что такое социальная инженерия в контексте информационной безопасности?
9. Опишите функции антивирусных средств.
10. Как работают средства резервного копирования?
11. Опишите технические средства защиты интеллектуальной собственности в электронной среде.

Раздел 4. Защита информации в телекоммуникационных сетях

1. Что такое сертификат сайта, как работает, откуда получить?
2. Какие существуют средства сетевой защиты устройств?
3. Охарактеризуйте основные особенности защиты информации в электронной почте и мессенджерах.
4. Опишите основные особенности распространения информации в телекоммуникационных сетях.
5. Опишите принципы построения единого пространства сети Интернет.
6. Опишите проблемы защиты приватности в телекоммуникационных сетях.
7. Опишите особенности защиты интеллектуальной собственности в сети Интернет.

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 по защите информации.
2. Современное законодательство РФ по защите интеллектуальной собственности.
3. Пример построения модели угроз образовательной организации.
4. Влияние развития квантовых вычислений на криптографию.
5. Влияние развития искусственного интеллекта на отрасль защиты информации.
6. Средства защиты информации в современных мобильных устройствах.
7. Проблемы защиты интеллектуальной собственности в эпоху развития искусственного интеллекта.
8. Альянс «Пять глаз» и аналогичные альянсы.
9. Современные антивирусные программы, их функции и возможности.
10. Проблема приватности пользователей в сети Интернет.
11. Средства защиты данных в современных мессенджерах.
12. Законодательные инициативы государств по усилению контроля за пользователями сети Интернет.
13. Современные персональные средства защиты конфиденциальной информации.
14. Современные методы мошенничества в сети Интернет.
15. Современные криптовалюты.

Шкала и критерии оценки доклада

Критерии	Показатели	Баллы
1. Степень раскрытия сущности проблемы	<ul style="list-style-type: none"> – 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	<ul style="list-style-type: none"> – 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

ОПК-5.2.1-1. 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

ОПК-5.2.1-2. 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:

--

ОПК-5.2.1-3. 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

--

ОПК-5.2.1-4. 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

--

ОПК-5.2.1-5. Прочитайте текст и установите соответствие.

Установите соответствие между категорией информации и ее определением:

<p>А. Конфиденциальность Б. Аутентичность В. Неотказуемость Г. Доступность</p>	<ol style="list-style-type: none"> 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

ОПК-5.2.2-1. 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

ОПК-5.2.2-2. 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

ОПК-5.2.2-3. Прочитайте текст и запишите развёрнутый обоснованный ответ.

Что такое хэш функция, для чего применяется?

--

ОПК-5.2.2-4. 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

ОПК-5.2.2-5. 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

ОПК-5.2.3-1. Прочитайте текст и запишите развёрнутый обоснованный ответ.

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

--

ОПК-5.2.3-2. Прочитайте текст и запишите развёрнутый обоснованный ответ.

Нарисуйте схему подписывания с использованием открытого и закрытого ключа:

--

ОПК-5.2.3-3. 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

ОПК-5.2.3-4. 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

ОПК-5.2.3-5. 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

ОПК-5.2.1-1	A2B5B1ГЗД4
ОПК-5.2.1-2	231
ОПК-5.2.1-3	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.
ОПК-5.2.1-4	В В случае пассивной атаки атакующий только прослушивает коммуникации, но не может на них влиять. Понятия «нейтральная» атака не существует.
ОПК-5.2.1-5	A2B4B1ДЗ
ОПК-5.2.2-1	АБГ Существует только три направления защиты информации. Остальные указанные пункты не относятся к направлениям защиты.
ОПК-5.2.2-2	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.
ОПК-5.2.2-3	Хэш функция – это алгоритм, преобразующий входные данные любого объема (файл, текст) в уникальную строку фиксированной длины (хэш-сумма). Она

	<p>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.</p>
ОПК-5.2.2-4	<p>БВЕ</p> <p>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.</p>
ОПК-5.2.2-5	<p>А</p> <p>Заражаться могут любые файлы, которые содержат инструкции для исполнения либо программного кода, либо инструкции для интерпретации некоторого кода, например, макросы или скрипты в документах.</p>
ОПК-5.2.3-1	<p>Открытый ключ используется для зашифрования</p> <p>Закрытый ключ используется для расшифрования</p> <p>Публикация открытого ключа</p> <p>Сервер открытых ключей</p> <p>Закрытый</p> <p>Открытый</p> <p>Получатель должен создать два связанных ключа</p>
ОПК-5.2.3-2	<p>Подпись верна или не верна</p> <p>Проверка ЭП</p> <p>Создание ЭП</p> <p>Открытый ключ используется для проверки ЭЦП</p> <p>Закрытый ключ используется для создания ЭЦП</p> <p>Публикация открытого ключа</p> <p>Сервер открытых ключей</p> <p>Закрытый</p> <p>Открытый</p> <p>Получатель должен создать два связанных ключа</p>
ОПК-5.2.3-3	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.
ОПК-5.2.3-4	АВ Создание и удаление являются частным случаем доступа на запись.
ОПК-5.2.3-5	<p>Создание подписи</p>  <p>Проверка подписи</p> 

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.