ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ

C=RU, S=Ставропольский край, L=г. Ставрополь, T=проректор по учебной работе, OU=ректорат, O="ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "" СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ""", СНИЛС=15230589951, ИНН=263411176761, E=s.a.maksimovich@stgau.ru, G=Светлана Александровна, SN=Максимович, CN=Максимович Светлана Александровна

УТВЕРЖДАЮ

Директор/Декан
факультета цифровых технологий
Шлаев Дмитрий Валерьевич

_____

_____

«___» _____ 20___ г.

Рабочая программа дисциплины

Б1.В.05 Управление информационной безопасностью

09.04.03 Прикладная информатика

Искусственный интеллект в кибербезопасности

магистр

очная

Ставрополь, 2026

1. Цель дисциплины

Целью освоения дисциплины «Информационная безопасность» является изучение и приобретение студентами комплексных знаний о принципах и закономерностях информационной безопасности.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций ОП ВО и овладение следующими результатами обучения по дисциплине:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Перечень планируемых результатов обучения по дисциплине
ПК-4 Способен администрировать средства защиты информации и обеспечивать безопасность информационных систем	ПК-4.1 Администрирует средства защиты информации прикладного и системного программного обеспечения (ОС, СУБД, приложения), настраивая политики безопасности и контролируя их соблюдение	**знает** средства защиты информации прикладного и системного программного обеспечения, политики информационной безопасности и порядок контроля их соблюдения **умеет** настраивать политики информационной безопасности и администрировать средства защиты информации **владеет навыками** навыками администрирования средств защиты информации и контроля соблюдения политик безопасности

3. Место дисциплины в структуре образовательной программы

Дисциплина «Управление информационной безопасностью» является дисциплиной части, формируемой участниками образовательных отношений программы.

Изучение дисциплины осуществляется в 1семестре(-ах).

Для освоения дисциплины «Управление информационной безопасностью» студенты используют знания, умения и навыки, сформированные в процессе изучения дисциплин:

Системы электронного документооборота

Программно-аппаратная защита информации

Ознакомительная практика

Теория информационных процессов и системБезопасность облачных технологий

Освоение дисциплины «Управление информационной безопасностью» является необходимой основой для последующего изучения следующих дисциплин:

Преддипломная практика

Администрирование безопасных информационных систем

Администрирование защищенных сетей

Технологии непрерывной разработки и безопасности

Поведенческий анализ и мониторинг защищенности с использованием ИИ

Обнаружение и анализ вредоносного программного обеспечения

Подготовка к сдаче и сдача государственного экзамена

Подготовка к процедуре защиты и защита выпускной квалификационной работы

Технологическая (проектно-технологическая) практика

Технологии разработки защищенного ПО

4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины «Управление информационной безопасностью» в соответствии с рабочим учебным планом и ее распределение по видам работ представлены ниже.

Семестр	Трудоемкость час/з.е.	Контактная работа с преподавателем, час			Самостоятельная работа, час	Контроль, час	Форма промежуточной аттестации (форма контроля)
		лекции	практические занятия	лабораторные занятия			
1	144/4	12	24		72	36	Эк
в т.ч. часов: в интерактивной форме		2	6				
практической подготовки		12	24		72		

Семестр	Трудоемкость час/з.е.	Внеаудиторная контактная работа с преподавателем, час/чел					
		Курсовая работа	Курсовой проект	Зачет	Дифференцированный зачет	Консультации перед экзаменом	Экзамен
1	144/4						0.25

5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

№	Наименование раздела/темы	Семестр	Количество часов					Формы текущего контроля успеваемости и промежуточной аттестации	Оценочное средство проверки результатов достижения индикаторов компетенций	Код индикаторов достижения компетенций
			всего	Лекции	Семинарские занятия		Самостоятельная работа			
					Практические	Лабораторные				
1.	1 раздел. 1									
1.1.	Общая характеристика информационной безопасности. Угроза (утечка) информации	1	10	2	8		12	КТ 1	Тест	ПК-4.1
1.2.	Уровни информационной безопасности	1	18	6	12		24	КТ 2	Тест	ПК-4.1
1.3.	Политика информационной без-опасности и формирование методов защиты информационных ресурсов	1	8	4	4		36	КТ 3	Тест	ПК-4.1
	Промежуточная аттестация	Эк								
	Итого		144	12	24		72			
	Итого		144	12	24		72			

5.1. Лекционный курс с указанием видов интерактивной формы проведения занятий

Тема лекции (и/или наименование раздел) (вид интерактивной формы проведения занятий)/ (практическая подготовка)	Содержание темы (и/или раздела)	Всего, часов / часов интерактивных занятий/ практическая подготовка
Общая характеристика информационной безопасности. Угроза (утечка) информации	Понятие информационной безопасности. основные составляющие. важность проблемы	2/2
Уровни информационной безопасности	Законодательный уровень информационной безопасности	2/-
Уровни информационной безопасности	Административный уровень информационной безопасности	2/-
Уровни информационной безопасности	Наиболее распространенные угрозы информационной безопасности	2/-
Политика информационной без-опасности и формирование методов защиты информационных ресурсов	Протоколирование и аудит, шифрование, контроль целостности	2/-
Политика информационной без-опасности и формирование методов защиты информационных ресурсов	Заключительная лекция	2/-
Итого		12

5.2.1. Семинарские (практические) занятия с указанием видов проведения занятий в интерактивной форме

Наименование раздела дисциплины	Формы проведения и темы занятий (вид интерактивной формы проведения занятий)/(практическая подготовка)	Всего, часов / часов интерактивных занятий/ практическая подготовка	
		вид	часы
Общая характеристика информационной безопасности. Угроза (утечка) информации	Организация и обеспечение безопасности (Каналы утечки ин-формации)	Пр	4/2/4
Общая характеристика информационной безопасности. Угроза (утечка) информации	Процедурный уровень информационной безопасности. Физическая защита	Пр	4/-/4
Уровни информационной безопасности	Организационно-правовые методы защиты информации на предприятиях	Пр	4/2/4

Уровни информационной безопасности	Проектирование уровней информационной безопасности	Пр	4/-/4
Уровни информационной безопасности	Информационная безопасность ПЭВМ	Пр	2/-/2
Уровни информационной безопасности	Информационные войны	Пр	2/2/2
Политика информационной без-опасности и формирование методов защиты информационных ресурсов	Криптография. Понятие о криптографической деятельности	Пр	2/-/2
Политика информационной без-опасности и формирование методов защиты информационных ресурсов	Управление доступом с помощью биометрических характеристик	Пр	2/-/2
Итого			

5.3. Курсовой проект (работа) учебным планом не предусмотрен

5.4. Самостоятельная работа обучающегося

Темы и/или виды самостоятельной работы	Часы
Изучение пройденного материала и подготовка к лабораторной работе	6
Изучение пройденного материала и подготовка к лабораторной работе	6
Изучение пройденного материала и подготовка к лабораторной работе	6
Изучение пройденного материала и подготовка к лабораторной работе	6

Изучение пройденного материала и подготовка к лабораторной работе	6
Изучение пройденного материала и подготовка к лабораторной работе	6
Изучение пройденного материала и подготовка к лабораторной работе	6
Изучение пройденного материала и подготовка к лабораторной работе	24
Подготовка к экзамену	6

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Учебно-методическое обеспечение для самостоятельной работы обучающегося по дисциплине «Управление информационной безопасностью» размещено в электронной информационно-образовательной сре-де Университета и доступно для обучающегося через его личный кабинет на сайте Университета. Учебно-методическое обеспечение включает:

1. Рабочую программу дисциплины «Управление информационной безопасностью».

2.Методические рекомендации для организации самостоятельной работы обучающегося по дисциплине «Управление информационной безопасностью».

3. Методические рекомендации по выполнению письменных работ () (при наличии).

4. Методические рекомендации по выполнению контрольной работы студентами заочной формы обучения (при наличии)

5. Методические указания по выполнению курсовой работы (проекта) (при наличии).

Для успешного освоения дисциплины, необходимо самостоятельно детально изучить представленные темы по рекомендуемым источникам информации:

№ п/п	Темы для самостоятельного изучения	Рекомендуемые источники информации (№ источника)		
		основная (из п.8 РПД)	дополнительная (из п.8 РПД)	метод. лит. (из п.8 РПД)
1	Общая характеристика информационной безопасности. Угроза (утечка) информации. Изучение пройденного материала и подготовка к лабораторной работе	Л1.1, Л1.2	Л2.1	
2	Общая характеристика информационной безопасности. Угроза (утечка) информации. Изучение пройденного материала и подготовка к лабораторной работе	Л1.1, Л1.2	Л2.1	
3	Уровни информационной безопасности. Изучение пройденного материала и подготовка к лабораторной работе	Л1.1, Л1.2	Л2.1	
4	Уровни информационной безопасности. Изучение пройденного материала и подготовка к лабораторной работе	Л1.1, Л1.2	Л2.1	
5	Уровни информационной безопасности. Изучение пройденного материала и подготовка к лабораторной работе	Л1.1, Л1.2	Л2.1	
6	Уровни информационной безопасности. Изучение пройденного материала и подготовка к лабораторной работе	Л1.1, Л1.2	Л2.1	
7	Политика информационной без-опасности и формирование методов защиты информационных ресурсов. Изучение пройденного материала и подготовка к лабораторной работе	Л1.1, Л1.2	Л2.1	
8	Политика информационной без-опасности и формирование методов защиты информационных ресурсов.	Л1.1, Л1.2	Л2.1	

	Изучение пройденного материала и подготовка к лабораторной работе			
9	Политика информационной безопасности и формирование методов защиты информационных ресурсов. Подготовка к экзамену	Л1.1, Л1.2	Л2.1	

7. Фонд оценочных средств (оценочных материалов) для проведения промежуточной аттестации обучающихся по дисциплине «Управление информационной безопасностью»

7.1. Перечень индикаторов компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Индикатор компетенции (код и содержание)	Дисциплины/элементы программы (практики, ГИА), участвующие в формировании индикатора компетен-ции	

7.2. Критерии и шкалы оценивания уровня усвоения индикатора компетенций, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Оценка знаний, умений и навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций по дисциплине «Управление информационной безопасностью» проводится в форме текущего контроля и промежуточной аттестации.

Текущий контроль проводится в течение семестра с целью определения уровня усвоения обучающимися знаний, формирования умений и навыков, своевременного выявления преподавателем недостатков в подготовке обучающихся и принятия необходимых мер по её корректировке, а также для совершенствования методики обучения, организации учебной работы и оказания индивидуальной помощи обучающемуся.

Промежуточная аттестация по дисциплине «Управление информационной безопасностью» проводится в виде Экзамен.

За знания, умения и навыки, приобретенные студентами в период их обучения, выставляются оценки «ЗАЧТЕНО», «НЕ ЗАЧТЕНО». (или «ОТЛИЧНО», «ХОРОШО», «УДОВЛЕТВОРИТЕЛЬНО», «НЕУДОВЛЕТВОРИТЕЛЬНО» для дифференцированного зачета/экзамена)

Для оценивания знаний, умений, навыков и (или) опыта деятельности в университете применяется балльно-рейтинговая система оценки качества освоения образовательной программы. Оценка проводится при проведении текущего контроля успеваемости и промежуточных аттестаций обучающихся. Рейтинговая оценка знаний является интегрированным показателем качества теоретиче-ских и практических знаний и навыков студентов по дисциплине.

Состав балльно-рейтинговой оценки студентов очной формы обучения

Для студентов очной формы обучения знания по осваиваемым компетенциям формируются на лекционных и практических занятиях, а также в процессе самостоятельной подготовки.

В соответствии с балльно-рейтинговой системой оценки, принятой в Университете студентам начисляются баллы по следующим видам работ:

№ контрольной точки	Оценочное средство результатов индикаторов достижения компетенций	Максимальное количество баллов
1 семестр		
КТ 1	Тест	10
КТ 2	Тест	10
КТ 3	Тест	10
Сумма баллов по итогам текущего контроля		**30**
Посещение лекционных занятий		20
Посещение практических/лабораторных занятий		20
Результативность работы на практических/лабораторных занятиях		30
Итого		100

№ контрольной точки	Оценочное средство результатов индикаторов достижений компетенций	Максимальное количество баллов	Критерии оценки знаний студентов
1 семестр			
КТ 1	Тест	10	10 баллов выставляется обучающемуся, если тестовые задания выполнены на 85 % и выше; 8–9 баллов выставляется обучающемуся, если тестовые задания выполнены на 70–84 %; 6–7 баллов выставляется обучающемуся, если тестовые задания выполнены на 55–69 %; 4–5 баллов выставляется обучающемуся, если тестовые задания выполнены на 44–54 %; 0–3 балла выставляется обучающемуся, если тестовые задания выполнены на 43 % и менее.
КТ 2	Тест	10	10 баллов выставляется обучающемуся, если тестовые задания выполнены на 85 % и выше; 8–9 баллов выставляется обучающемуся, если тестовые задания выполнены на 70–84 %; 6–7 баллов выставляется обучающемуся, если тестовые задания выполнены на 55–69 %; 4–5 баллов выставляется обучающемуся, если тестовые задания выполнены на 44–54 %; 0–3 балла выставляется обучающемуся, если тестовые задания выполнены на 43 % и менее.
КТ 3	Тест	10	10 баллов выставляется обучающемуся, если тестовые задания выполнены на 85 % и выше; 8–9 баллов выставляется обучающемуся, если тестовые задания выполнены на 70–84 %; 6–7 баллов выставляется обучающемуся, если тестовые задания выполнены на 55–69 %; 4–5 баллов выставляется обучающемуся, если тестовые задания выполнены на 44–54 %; 0–3 балла выставляется обучающемуся, если тестовые задания выполнены на 43 % и менее.

Критерии и шкалы оценивания результатов обучения на промежуточной аттестации

При проведении итоговой аттестации «зачет» («дифференцированный зачет», «экзамен») преподавателю с согласия студента разрешается выставлять оценки («отлично», «хорошо», «удовлетворительно», «зачет») по результатам набранных баллов в ходе текущего контроля успеваемости в семестре по выше приведенной шкале.

В случае отказа – студент сдает зачет (дифференцированный зачет, экзамен) по приведенным выше вопросам и заданиям. Итоговая успеваемость (зачет, дифференцированный зачет, экзамен) не может оцениваться ниже суммы баллов, которую студент набрал по итогам текущей и промежуточной успеваемости.

При сдаче (зачета, дифференцированного зачета, экзамена) к заработанным в течение семестра студентом баллам прибавляются баллы, полученные на (зачете, дифференцированном зачете, экзамене) и сумма баллов переводится в оценку.

Критерии и шкалы оценивания ответа на экзамене

Сдача экзамена может добавить к текущей балльно-рейтинговой оценке студентов не более 20 баллов:

Содержание билета	Количество баллов
Теоретический вопрос №1	до 7
Теоретический вопрос №2	до 7
Задача (оценка умений и	до 6
Итого	20

Критерии оценки ответа на экзамене

Теоретические вопросы (вопрос 1, вопрос 2)

7 баллов выставляется студенту, полностью освоившему материал дисциплины или курса в соответствии с учебной программой, включая вопросы рассматриваемые в рекомендованной программой дополнительной справочно-нормативной и научно-технической литературы, свободно владеющему основными понятиями дисциплины. Требуется полное понимание и четкость изложения ответов по экзаменационному заданию (билету) и дополнительным вопросам, заданных экзаменатором. Дополнительные вопросы, как правило, должны относиться к материалу дисциплины или курса, не отраженному в основном экзаменационном задании (билете) и выявляют полноту знаний студента по дисциплине.

5 балла заслуживает студент, ответивший полностью и без ошибок на вопросы экзаменационного задания и показавший знания основных понятий дисциплины в соответствии с обязательной программой курса и рекомендованной основной литературой.

3 балла дан недостаточно полный и недостаточно развернутый ответ. Логика и последовательность изложения имеют нарушения. Допущены ошибки в раскрытии понятий, употреблении терминов. Студент не способен самостоятельно выделить существенные и несущественные признаки и причинно-следственные связи. Студент может конкретизировать обобщенные знания, доказав на примерах их основные положения только с помощью преподавателя. Речевое оформление требует поправок, коррекции.

2 балла дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь данного понятия, теории, явления с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента не только на поставленный вопрос, но и на другие вопросы дисциплины.

1 балл дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях. Присутствуют фрагментарность, нелогичность изложения. Студент не осознает связь данного понятия, теории, явления с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента не только на поставленный вопрос, но и на другие вопросы дисциплины.

0 баллов - при полном отсутствии ответа, имеющего отношение к вопросу.

Оценивание задачи

6 баллов Задачи решены в полном объеме с соблюдением необходимой последовательности.

5 баллов Задачи решены с небольшими недочетами.

4 балла Задачи решены с небольшими недочетами.

3 балла Задачи решены не полностью, но объем выполненной части таков, что позволяет получить правильные результаты и выводы.

2 балла Задачи решены не полностью, но объем выполненной части таков, что позволяет получить правильные результаты и выводы.

1 баллов Задачи решены частично, с большим количеством вычислительных ошибок, объем выполненной части работы не позволяет сделать правильных выводов.

0 баллов Задачи не решены или работа выполнена не полностью, и объем выполненной части работы не позволяет сделать правильных выводов.

Перевод рейтинговых баллов в пятибалльную систему оценки знаний обучающихся:

для экзамена:

- «отлично» – от 89 до 100 баллов – теоретическое содержание курса освоено полностью, без пробелов необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному;

- «хорошо» – от 77 до 88 баллов – теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками;

- «удовлетворительно» – от 65 до 76 баллов – теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки;

- «неудовлетворительно» – от 0 до 64 баллов - теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над материалом курса не приведет к существенному повышению качества выполнения учебных заданий

7.3. Примерные оценочные материалы для текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины «Управление информационной безопасностью»

Вопросы для подготовки к экзамену

1. Дайте характеристику понятие секретной информации.
2. Охарактеризуйте понятие коммерческой тайны.
3. Что такое разрушение информации?
4. Методы уменьшения опасности компьютерных вирусов.
5. Классификация информации по уровню доступа.
6. Что такое открытая информация?
7. Что такое информация ограниченного доступа?
8. Конфиденциальность информации.
9. Целостность информации.
10. Доступность информации.
11. Понятие информационной безопасности.
12. Основные составляющие информационной безопасности.
13. Законодательный уровень информационной безопасности.
14. Обзор российского законодательства в области информационной безопасности.
15. Обзор зарубежного законодательства в области информационной безопасности.
16. Основные классы мер процедурного уровня.
17. Информационная инфраструктура.
18. Основные классы мер процедурного уровня.

19. Физическая защита.
20. Критичные ресурсы.
21. Реагирование на нарушения режима безопасности.
22. Основные понятия административного уровня ИБ.
23. Программа безопасности.
24. Политика безопасности.
25. Политика безопасности нижнего уровня.
26. Синхронизация программы безопасности с жизненным циклом систем.
27. Контроль деятельности в области безопасности.
28. Охарактеризуйте понятие АС.
29. Охарактеризуйте информационную безопасность.
30. Охарактеризуйте понятие угрозы информационной безопасности.
31. Классификация угроз по природе возникновения.
32. Классификация угроз по степени преднамеренности возникновения.
33. Классификация угроз по положению источника.
34. Классификация угроз по степени воздействия на АС.
35. Технические каналы утечки информации.
36. Функциональные каналы утечки информации и условия их образования.
37. Специальные каналы утечки информации и механизмы их возникновения.
38. Процедурный уровень информационной безопасности.
39. Физическая защита информации.
40. Анализ угроз ИБ объекта.
41. Методы и средства обеспечения ИБ на объектах связи специального назначения.
42. Модели нарушителя и угроз безопасности объекта.
43. Методы и средства ограничения доступа к информации и компонентам ЭВМ.
44. Привязка программного обеспечения к аппаратному окружения и физическим носителям.
45. Защита компьютерной информации и компьютерных систем от вредоносных программ.
46. История криптографии.
47. Простейшие шифры и их свойства. Стойкость шифров. Композиции шифров. Влияние криптографических средств на информационную безопасность.
48. Проблемы и методы информационной войны.
49. Методы иностранных технических разведок по ведению информационной войны их возможности.

1. Управление информационной безопасностью в современных организациях.
2. Политика информационной безопасности: назначение, структура и содержание.
3. Администрирование средств защиты информации прикладного программного обеспечения.
4. Администрирование средств защиты информации системного программного обеспечения.
5. Настройка политик безопасности в информационных системах.
6. Контроль соблюдения требований информационной безопасности.
7. Управление доступом пользователей к информационным ресурсам.
8. Средства защиты операционных систем, баз данных и приложений.
9. Организация мониторинга событий информационной безопасности.
10. Риски нарушения политик информационной безопасности.
11. Методы оценки эффективности средств защиты информации.
12. Документирование процессов управления информационной безопасностью.
13. Роль искусственного интеллекта в управлении информационной безопасностью.
14. Автоматизация контроля соблюдения политик безопасности.
15. Совершенствование системы управления информационной безопасностью организации.

Примерные вопросы для устного опроса:

1. Что понимается под управлением информационной безопасностью?
2. Какие задачи решает политика информационной безопасности?

3. Какие средства защиты информации применяются в информационных системах?
4. Как выполняется настройка политик безопасности?
5. Для чего применяется контроль соблюдения политик безопасности?
6. Какие угрозы возникают при нарушении требований информационной безопасности?
7. Как организуется управление доступом пользователей?
8. Какие средства защиты применяются для операционных систем?
9. Как обеспечивается безопасность прикладного программного обеспечения?
10. Какую роль играет мониторинг событий информационной безопасности?
11. Как оценивается эффективность средств защиты информации?
12. Как искусственный интеллект может использоваться в управлении информационной безопасностью?

Примерные тестовые задания:

1. Политика информационной безопасности предназначена для:
а) установления правил защиты информации и порядка их соблюдения;
б) удаления всех информационных ресурсов;
в) отказа от контроля доступа;
г) замены всех пользователей.
Правильный ответ: а.

2. Администрирование средств защиты информации включает:
а) настройку, сопровождение и контроль работы защитных механизмов;
б) только удаление программного обеспечения;
в) отказ от обновлений;
г) отключение всех средств защиты.
Правильный ответ: а.

3. Контроль соблюдения политик безопасности необходим для:
а) выявления нарушений и поддержания защищенности информационных систем;
б) отмены требований безопасности;
в) передачи паролей всем пользователям;
г) удаления журналов событий.
Правильный ответ: а.

4. Управление доступом пользователей направлено на:
а) разграничение прав доступа к информационным ресурсам;
б) открытие всех данных для всех пользователей;
в) удаление учетных записей без анализа;
г) отказ от идентификации.
Правильный ответ: а.

5. Мониторинг событий информационной безопасности используется для:
а) обнаружения подозрительной активности и нарушений безопасности;
б) замены всех документов;
в) удаления средств защиты;
г) отключения информационной системы.
Правильный ответ: а.

Примерные практические задания:

1. Составить структуру политики информационной безопасности организации.
2. Определить требования к настройке политик безопасности для информационной системы.
3. Описать порядок администрирования средств защиты информации.
4. Составить схему разграничения доступа пользователей к информационным ресурсам.

5. Проанализировать возможные нарушения политики информационной безопасности.

6. Предложить меры контроля соблюдения требований безопасности.

7. Составить перечень событий, подлежащих мониторингу в системе безопасности.

8. Оценить возможности применения искусственного интеллекта для контроля информационной безопасности.

8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

а) Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

основная

Л1.1 Гришина Н. В. Информационная безопасность предприятия [Электронный ресурс]:Учебное пособие; ВО - Бакалавриат. - Москва: Издательство "ФОРУМ", 2016. - 239 с. – Режим доступа: http://new.znanium.com/go.php?id=544554

Л1.2 Башлы П. Н., Бабаш А. В. Информационная безопасность и защита информации [Электронный ресурс]:учебник ; ВО - Бакалавриат. - Москва: Издательский Центр РИО□, 2013. - 222 с. – Режим доступа: http://new.znanium.com/go.php?id=405000

дополнительная

Л2.1 Озерский С. В., Попов Информационная безопасность [Электронный ресурс]:практикум ; ВО - Бакалавриат, Специалитет. - Самара: Самарский юридический институт ФСИН России, 2019. - 84 с. – Режим доступа: http://znanium.com/go.php?id=1094244

9. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

№	Наименование ресурса сети «Интернет»	Электронный адрес ресурса
1	Информационная безопасность	https://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf
2	Информационная безопасность	http://elar.uspu.ru/bitstream/uspu/4122/1/uch00029.pdf
3	Информационная безопасность	

10. Методические указания для обучающихся по освоению дисциплины

Лекционные занятия

Основа освоения дисциплины – лекция, целью которой является целостное и логичное рассмотрение основного материала курса. Вместе с тем значимость лекции определяется тем, что она не только способствует выработке логического мышления, но и способствует развитию интереса к пониманию современной действительности.

Задача студентов в процессе умелой и целеустремленной работы на лекциях –внимательно слушать преподавателя, следить за его мыслью, предлагаемой системой логических посылок, доказательств и выводов, фиксировать (записывать) основные идеи, важнейшие характеристики понятий, теорий, наиболее существенные факты. Лекция задает направление, содержание и эффективность других форм учебного процесса, нацеливает студентов на самостоятельную работу и определяет основные ее направления (подготовку к практическим занятиям, выполнение творческих заданий, рефератов, решение контекстных задач).

Записывание лекции – творческий процесс. Запись лекции крайне важна. Это позволяет надолго сохранить основные положения лекции; способствует поддержанию внимания; способствует лучшему запоминания материала. Важно уметь оформить конспект так, чтобы важные моменты были выделены графически, а главную информацию следует выделять в самостоятельные абзацы, фиксируя ее более крупными буквами или цветными маркерами. Конспект должен иметь поля для заметок. Это могут быть библиографические ссылки и, наконец, собственные

комментарии. Для быстрой записи теста можно придумать условные знаки, при этом таких знаков не должно быть более 10–15. Условные обозначения придумывают для часто встречающихся слов (существует, который, каждый, точка зрения, на основании и т.п.).

Перед каждой лекцией необходимо внимательно прочитать материал предыдущей лекции. В рабочей тетради графически выделить: тему лекции, основные теоретические положения. Подготовленный студент легко следит за мыслью преподавателя, что позволяет быстрее запоминать новые понятия, сущность которых выявляется в контексте лекции. Повторение материала облегчает в дальнейшем подготовку к зачету. Затем надо ознакомиться с материалом темы по учебнику, внести нужные уточнения и дополнения в лекционный материал. После усвоения каждой темы рекомендуется проверять свои знания, отвечая на контрольные вопросы по теме.

Практические занятия

Целью практических занятий является закрепление, расширение, углубление теоретических знаний, полученных на лекциях и в ходе самостоятельной работы, развитие познавательных способностей.

Являясь частью образовательного процесса, семинар преследует ряд основополагающих задач:

- работа с источниками, которая идет на уровнях индивидуальной самостоятельной работы и в ходе коллективного обсуждения;
- формирование умений и навыков индивидуальной и коллективной работы, позволяющих эффективно использовать основные методы исследования, грамотно выстраивать его основные технологические этапы (знакомство с темой и имеющейся по ней информацией, определение основной проблемы, первичный анализ, определение подходов и ключевых узлов механизма ее развития, публичное обсуждение, предварительные выводы);
- анализ поставленных проблем, умение обсуждать тему, высказывать свое мнение, отстаивать свою позицию, слушать и оценивать различные точки зрения, конструктивно полемизировать, учиться думать, говорить, слушать, понимать, находить точки соприкосновения разных позиций, их разумного сочетания;
- формирование установок на творчество;
- диалог, внутренний и внешний; поиск и разрешение проблемы в рамках имеющейся о ней информации;
- поиск рационального зерна в самых противоречивых позициях и подходах к проблеме;
- открытость новому и принципиальную возможность изменить свою позицию и вытекающие из нее решения, в случае получения новой информации и связанных с ней обстоятельств сознательный отход от подготовленного к семинару текста во время своего, построенного на тезисном изложении фактов и мыслей, когда конспект привлекается лишь в том случае, когда надо привести какие-то факты.

Для эффективной работы на практическом занятии студенту необходимо учесть и выполнить следующие требования по подготовке к нему:

1. Внимательно прочитать, как сформулирована тема, определить ее место в учебном плане курса, установить взаимосвязи с другими разделами.
2. Познакомиться с целью и задачами работы на практическом занятии, обратив внимание на то, какие знания, умения и навыки студент должен приобрести в результате активной познавательной деятельности.
3. Проработать основные вопросы и проблемы (задания), которые будут рассматриваться и обсуждаться в ходе практического занятия.
4. Подобрать литературу по теме занятия; найти соответствующий раздел в лекциях и в рекомендуемых пособиях.
5. Добросовестно проработать имеющуюся научную литературу (просмотреть и подобрать информацию, сделать выписки (конспектирование узловых проблем), обработать их в соответствии с задачами практического занятия.
6. Обдумать и предложить свои выводы и мысли на основании полученной информации (предварительное осмысление).
7. Продумать развернутые законченные ответы на предложенные вопросы, предлагаемые творческие задания и контекстные задачи, опираясь на материал лекций, расширяя и дополняя его данными из учебника, дополнительной литературы, составить план ответа, выписать

терминологию.

Видами заданий на практических занятиях:

- для овладения знаниями: чтение текста (учебника, первоисточника, дополнительной литературы), работа со словарями и справочниками, ознакомление с нормативными документами, учебно-исследовательская работа, использование аудио- и видеозаписей, компьютерной техники и Интернета и др.

- для закрепления и систематизации знаний: работа с конспектом лекции, обработка текста, повторная работа над учебным материалом (учебника, первоисточника, дополнительной литературы, аудио и видеозаписей, ответы на контрольные вопросы, аналитическая обработка текста, подготовка мультимедиа сопровождения к защите рефератов, и др.

- для формирования умений: решение контекстных задач, подготовка к деловым играм, выполнение творческих заданий, анализ профессиональных умений с использованием аудио- и видео-техники и др.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства и информационных справочных систем (при необходимости).

11.1 Перечень лицензионного программного обеспечения

1. Kaspersky Endpoint Security 12.11 - Антивирус
2. Microsoft Windows Server STDCORE AllLngLicense/Software AssurancePack Academic OLV 16Licenses LevelE AdditionalProduct CoreLic 1Year - Серверная операционная система

11.3 Перечень программного обеспечения отечественного производства

1. Kaspersky Endpoint Security 12.11 - Антивирус

При осуществлении образовательного процесса студентами и преподавателем используются следующие информационно справочные системы: СПС «Консультант плюс», СПС «Гарант».

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

№ п/п	Наименование специальных помещений и помещений для самостоятельной работы	Номер аудитории	Оснащенность специальных помещений и помещений для самостоятельной работы
1	Учебная аудитория для проведения занятий всех типов (в т.ч. лекционного, семинарского, практической подготовки обучающихся), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Э-160	Специализированная мебель на 180 посадочных мест, персональный компьютер – 1 шт., проектор Panasonic EX620 X6A – 1 шт., интерактивная доска SMART Board 690 – 1 шт., трибуна для лектора – 1 шт., микрофон – 1 шт., мониторы - 3 шт., плазменная панель - 1 шт., учебно-наглядные пособия в виде презентаций, информационные плакаты, подключение к сети «Интернет», выход в корпоративную сеть университета.

		Э-182	Оснащение: специализированная мебель на 14 посадочных мест, рабочие станции 13 шт., проектор Panasonic PT-LB55NTE – 1 шт., интерактивная доска SMART Board 690 – 1 шт., учебно-наглядные пособия в виде презентаций, подключение к сети «Интернет», доступ в электронную информационно-образовательную среду университета, выход в корпоративную сеть университета.
2	Помещение для самостоятельной работы обучающихся, подтверждающее наличие материально-технического обеспечения, с перечнем основного оборудования		

13. Особенности реализации дисциплины лиц с ограниченными возможностями здоровья

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники и учебные пособия, иная учебная литература, специальные технические средства обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

а) для слабовидящих:

- на промежуточной аттестации присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);
- задания для выполнения, а также инструкция о порядке проведения промежуточной аттестации оформляются увеличенным шрифтом;
- задания для выполнения на промежуточной аттестации зачитываются ассистентом;
- письменные задания выполняются на бумаге, надиктовываются ассистенту;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- студенту для выполнения задания при необходимости предоставляется увеличивающее устройство;

в) для глухих и слабослышащих:

- на промежуточной аттестации присутствует ассистент, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (он помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе записывая под диктовку);
- промежуточная аттестация проводится в письменной форме;
- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости поступающим предоставляется звукоусиливающая аппаратура индивидуального пользования;
- по желанию студента промежуточная аттестация может проводиться в письменной форме;

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

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;
- по желанию студента промежуточная аттестация проводится в устной форме.

Рабочая программа дисциплины «Управление информационной безопасностью» составлена на основе Федеральный государственный образовательный стандарт высшего образования - магистратура по направлению подготовки 09.04.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 916).

Автор (ы)

_____ доцент , к.т.н. Трошков А.М.

Рецензенты

_____ доцент , к.т.н. Рачков В.Е.

_____ профессор , д.э.н. Шуваев А.В.

Рабочая программа дисциплины «Управление информационной безопасностью» рассмотрена на заседании Кафедра информационных систем протокол № 9 от 07.04.2026 г. и признана соответствующей требованиям ФГОС ВО и учебного плана по направлению подготовки 09.04.03 Прикладная информатика

Заведующий кафедрой _____ Хабаров А.Н.

Рабочая программа дисциплины «Управление информационной безопасностью» рассмотрена на заседании учебно-методической комиссии Факультет цифровых технологий протокол № 2 от 08.04.3036 г. и признана соответствующей требованиям ФГОС ВО и учебного плана по направлению подготовки 09.04.03 Прикладная информатика

Руководитель ОП _____