Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Северо-Осетинский государственный университет
имени Коста Левановича Хетагурова»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Информационная безопасность»

Специальность 38.05.01 Экономическая безопасность

Специализация «Экономико-правовое обеспечение экономической безопасности»

Квалификация (степень) выпускника – экономист

Форма обучения
очная

Владикавказ 2019

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по специальности 38.05.01 Экономическая безопасность (уровень специалитета), утвержденным приказом Министерства образования и науки Российской Федерации от 16.01.2017 г., №20, учебным планом подготовки специалиста по направлению 38.05.01 Экономическая безопасность специализация «Экономико-правовое обеспечение экономической безопасности», одобренным Ученым советом ФГБОУ ВО «СОГУ» 28.05.2019 г., протокол № 10 и утвержденным ректором ФГБОУ ВО «СОГУ» А.У. Огоевым 28.05.2019 г.

Составитель: Биткина В.В.

Программа обсуждена на заседании кафедры прикладной математики

Одобрена Советом факультета экономики и управления

(протокол № 5 от 21.03.2019 г.)

Рабочая программа одобрена в составе основной профессиональной образовательной программы по специальности 38.05.01 Экономическая безопасность специализация «Экономико-правовое обеспечение экономической безопасности» решением Ученого совета ФГБОУ ВО «СОГУ»

(протокол №10 от 28.05.2019 г.)

1. Структура, и общая трудоемкость дисциплины

Общая трудоемкость дисциплины составляет 2 зачетные единицы (72 часа).
Форма промежуточной аттестации – зачет.

	Очная форма обучения
Курс	4
Семестр	8
Лекции	16
Практические (семинарские) занятия	-
Лабораторные занятия	32
Итого аудиторных занятий,	48
Самостоятельная работа	24
Курсовая работа	-
Экзамен	-
Зачет	+
Общее количество часов	72 / 2 зет

2. Цели освоения дисциплины

Целью освоения дисциплины «Информационная безопасность» является обеспечение освоения студентами сущности информационной безопасности, ее структуры и объектов и основных направлений обеспечения безопасности.

3. Место дисциплины в структуре ОПОП

Б1.В.02.

Дисциплина «Информационная безопасность» является дисциплиной вариативной части Блока 1 учебного плана подготовки специалиста по специальности 38.05.01 Экономическая безопасность, специализации «Экономико-правовое обеспечение экономической безопасности».

Для изучения курса необходимо знание дисциплин «Информационные технологии», «Информационные системы в юриспруденции», «Информационные системы в экономике».

4. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Коды компетенций	Содержание компетенций
ОК-12	способность работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации
ПК-20	способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности

ПК-28	способность осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач
ПК-29	способность выбирать инструментальные средства для обработки финансовой, бухгалтерской и иной экономической информации и обосновывать свой выбор
ПК-32	способность проводить анализ возможных экономических рисков и давать им оценку, составлять и обосновывать прогнозы динамики развития основных угроз экономической безопасности

Взаимосвязь планируемых результатов обучения по дисциплине с формируемыми компетенциями ОПОП

Коды компе-тенций	**Планируемые результаты обучения, соответствующие формируемым компетенциям ОПОП**		
	Знать	Уметь	Владеть
ОК-12	- принципы и методы работы с информацией, информационными ресурсами, основные информационные системы и технологии;	- применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации; - применять автоматизированные информационные системы и технологии при решении профессиональных задач;	- основными методами, способами и средствами получения, хранения, поиска, систематизации, обработки и передачи информации; навыками применения автоматизированных информационных систем и технологий при решении профессиональных задач;
ПК-20	- требования, установленные нормативными правовыми актами в области защиты государственной тайны; - основы разработки, оформления и ведения служебных документов; - основы информационной безопасности, способы	- соблюдать режим секретности. - использовать нормативные правовые документы в своей профессиональной деятельности. - анализировать и обобщать служебную информацию по степени ее конфиденциальности	- навыками применять действующее законодательство в профессиональной деятельности; - приемами обеспечения и соблюдения режима секретности; - способностью соблюдать в профессиональной деятельности требования, установленные

	соблюдения режима секретности;		нормативными правовыми актами в области защиты государственной тайны и информационной безопасности
ПК-28	- основные положения законодательных и правовых актов, регулирующих защиту государственной тайны и информационной безопасности;	- применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации;	- основными методами, способами и средствами получения, хранения, поиска, систематизации, обработки и передачи информации; навыками применения автоматизированных информационных систем и технологий при решении профессиональных задач;
ПК-29	- принципы и методы работы с информацией, информационными ресурсами, основные информационные системы и технологии;	- применять автоматизированные информационные системы и технологии при решении профессиональных задач;	- основными методами, способами и средствами получения, хранения, поиска, систематизации, обработки и передачи информации; навыками применения автоматизированных информационных систем и технологий при решении профессиональных задач;
ПК-32	- основы организации защиты государственной тайны в РФ в целом, а также в организациях и учреждениях.	- использовать в профессиональной деятельности нормативные правовые акты в области защиты государственной тайны и информационной безопасности, а также нормативные методические документы;	- навыками обеспечения защиты государственной тайны и соблюдения режима секретности в процессе профессиональной деятельности.

5. Содержание и учебно-методическая карта дисциплины

Таблица 5.1

Номер недели	Наименование тем (вопросов), изучаемых по дисциплине	Занятия		Самостоятельная работа студентов		Формы контроля	Литература
		л	лаб	Содержание	Часы		
1	Тема 1: Информационное общество. Информатизация общества (ОК-12, ПК-20, ПК-28, ПК-29,ПК-32)	2				Опрос	[2]
1,2	Тема 2: Понятие информации. Подходы к измерению информации. (ОК-12, ПК-28, ПК-29)		4			Опрос, проверка выполненных заданий	[6]
3	Тема 3: Понятие информационной безопасности (ОК-12, ПК-20, ПК-28, ПК-29,ПК-32)	2				Опрос	[2]
3,4	Тема 4: Кодирование текстовой и графической информации. (ОК-12, ПК-28, ПК-29)		4			Опрос, проверка выполненных заданий	[6]
5	Тема 5: Информационно-техническая и информационно-психологическая безопасности (ОК-12, ПК-28, ПК-29,ПК-32)	2				Опрос	[2]
5,6	Тема 6: Кодирование числовой информации (ОК-12, ПК-28, ПК-29)		4	Система QR-кодов	4	Опрос, проверка выполненных заданий	[6]
7	Тема 7: Теоретические и методологические вопросы организационного и правового обеспечения информационной безопасности (ОК-12, ПК-20, ПК-28, ПК-29,ПК-32)	2		Организационное обеспечение информационной безопасности Российской Федерации	4	Опрос	[1]

7,8	Тема 8: Шифрование. Виды шифров. (ОК-12, ПК-28, ПК-29)		4	Исторические шифры	4	Опрос, проверка выполненных заданий	[5]
9	Тема 9: Уголовная ответственность за посягательства на информационную безопасность (ОК-12, ПК-20, ПК-28, ПК-29,ПК-32)	2		Информация как предмет уголовно-правовой охраны	4	Опрос	[3]
9, 10	Тема 10: Шифр RSA (ОК-12, ПК-28, ПК-29)		4			Опрос, проверка выполненных заданий	[5]
11	Тема 11: Информационная безопасность в предпринимательской деятельности (ОК-12, ПК-20, ПК-28, ПК-29,ПК-32)	2				Опрос	[4]
11, 12	Тема 12: Хеш-функция (ОК-12, ПК-28, ПК-29)		4			Опрос, проверка выполненных заданий	[4]
13	Тема 13: Банковская система Российской Федерации. Концепция безопасности коммерческого банка (ОК-12, ПК-28, ПК-29,ПК-32)	2				Опрос	[4]
13, 14	Тема 14: Электронно-цифровая подпись (ОК-12, ПК-28, ПК-29,ПК-32)		4			Опрос, проверка выполненных заданий	[4]
15	Тема 15: Единый подход к защите информации в финансовой сфере (ОК-12, ПК-20, ПК-28, ПК-29,ПК-32)	2		Безопасность электронных банковских систем	4	Опрос	[4]
15, 16	Тема 16: Программное обеспечение для контроля подлинности документов. (ОК-12, ПК-28, ПК-29,ПК-32)		4	Полиграфические и голографические методы защиты от фальсификации документов и ценных бумаг	4	Опрос, проверка выполненных заданий	[4]

	ИТОГО:	**16**	**32**		**24**		

Примечание:

Отдельные виды учебной работы могут проводиться дистанционно на основании локальных нормативных актов.

При использовании индивидуальных образовательных траекторий в рамках индивидуального учебного плана подготовки специалиста изучение данной дисциплины может осуществляться через индивидуальные консультации преподавателя очно, в часы консультаций, по электронной почте, а также с использованием платформы дистанционного обучения Moodle, личный кабинет студента на сайте СОГУ, других элементов ЭИОС СОГУ.

6. Образовательные технологии

Для достижения планируемых результатов освоения дисциплины, используются различные образовательные технологии:

- традиционные лекции и лабораторные занятия с использованием современных интерактивных технологий;
- лекция-диалог – содержание подается через серию вопросов, на которые студент должен отвечать непосредственно в ходе лекции;
- видеоконференция – сеанс видеоконференцсвязи (ВКС) – это технология интерактивного взаимодействия двух и более участников образовательного процесса для обмена информацией в реальном режиме времени.

Технологии электронного обучения реализуются при помощи электронной образовательной среды СОГУ (при использовании ресурсов ЭБС), в ходе проведения автоматизированного тестирования и т.д.

7. Методические указания по дисциплине «Информационная безопасность»

7.1. Учебно-методическое обеспечение самостоятельной работы

Самостоятельная работа обучающихся является одним из видов учебных занятий. Самостоятельная работа проводится с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений обучающихся;
- углубления и расширения теоретических знаний;
- формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- формирования самостоятельности мышления, способности к саморазвитию, самосовершенствованию и самореализации;
- развития и закрепления исследовательских умений.

Самостоятельная работа обучающихся осуществляется на протяжении изучения всей дисциплины. В соответствии с утвержденной в учебном плане трудоемкостью она составляет 24 часа и состоит из:

- работы студентов с лекционными материалами, поиска и анализа литературы и электронных источников информации по заданной теме;
- выполнения заданий для самостоятельной работы в ЭИОС СОГУ;
- решения задач;
- изучения теоретического материала для подготовки к лабораторным занятиям; подготовки к зачету.

Темы и формы внеаудиторной самостоятельной работы, ее трудоёмкость содержатся в разделе 5, табл. 5.1.

7.2. Методические указания по проведению лабораторных занятий по дисциплине

Практические занятия призваны научить студента самостоятельно работать с учебными текстами, анализировать материал. В начале занятия рекомендуется рассмотреть соответствующий теоретический материал. Затем идет практический разбор изучаемого материала, решаются задачи, разбирается каждый конкретный пример.

В начале практического занятия следует обратить внимание на теоретические вопросы по теме занятия. Первоначально идет изложение теоретического материала темы занятия. Затем в ряде вопросов преподавателя следует сконцентрировать внимание на основных идеях темы занятия. Вопросы должны включать в себя различные вариации элементарных ситуаций, отображающих основные идеи темы занятия в их взаимосвязи. Задаваемые вопросы должны быть конкретными и максимально проявлять в студентах их сообразительность.

Устный опрос требует большой предварительной подготовки: тщательного отбора содержания, всестороннего продумывания вопросов, задач и примеров, которые будут предложены, путей активизации деятельности всех студентов группы в процессе проверки, создания на занятии деловой и доброжелательной обстановки.

Различают фронтальный, индивидуальный и письменный опрос.

Фронтальный опрос проводится в форме беседы преподавателя с группой. Он органически сочетается с повторением пройденного материала, являясь средством для закрепления знаний и умений. Его достоинство в том, что в активную умственную работу можно вовлечь всех студентов группы. Для этого вопросы должны допускать краткую форму ответа, быть лаконичными, логически взаимосвязанными друг с другом, даны в такой последовательности, чтобы ответы студентов в совокупности могли раскрыть содержание раздела, темы. С помощью фронтального опроса преподаватель имеет возможность проверить выполнение студентами домашнего задания, выяснить готовность группы к изучению нового материала, определить степень усвоения нового учебного материала, который был только что разобран на занятии.

Индивидуальный опрос предполагает обстоятельные, связные ответы студентов на вопрос, относящийся к изучаемому учебному материалу, поэтому он служит важным учебным средством развития речи, памяти, мышления обучающихся. Чтобы сделать такую проверку более глубокой, необходимо ставить перед студентами вопросы, требующие развернутого ответа.

Вопросы для индивидуального опроса должны быть четкими, ясными, конкретными, емкими, иметь прикладной характер, охватывать основной, ранее пройденный материал программы. Их содержание должно стимулировать студентов логически мыслить, сравнивать, анализировать, доказывать, подбирать убедительные примеры, устанавливать причинно-следственные связи, делать обоснованные выводы и этим способствовать объективному выявлению знаний студентов.

Вопрос обычно задают всей группе и после небольшой паузы, необходимой для того, чтобы студенты поняли его и приготовились к ответу, вызывают для ответа конкретного студента.

Письменная проверка наряду с устной является важнейшим методом контроля знаний, умений и навыков студентов. Однородность работ, выполняемых студентами, позволяет предъявлять ко всем одинаковые требования и обеспечивает объективность оценки результатов обучения. Применение этого метода дает возможность в наиболее короткий срок одновременно проверить усвоение учебного материала всеми студентами группы, определить направления для индивидуальной работы с каждым.

Письменная проверка используется во всех видах контроля и осуществляется как в аудиторной, так и во внеаудиторной работе (выполнение домашних заданий).

7.3. Методические рекомендации по использованию информационно-коммуникационных технологий обучения

Для изучения лекционного материала дисциплины могут применяться аудиовизуальные (мультимедийные) технологии, которые не отрицают традиционные, проверенные временем методы преподавания, но, при этом, они повышают наглядность, информативность, оперативность в подаче информации, позволяют экономить время занятий.

Каждое семинарское занятие имеет свою особую форму проведения, свою методологическую специфику, что позволяет развивать у студентов различные общекультурные, общепрофессиональные и профессиональные компетенции. Постановка проблемы, разбор актуальных конкретных и гипотетических ситуаций, создание атмосферы диалога между преподавателем и группой позволяет работать индивидуально и в малых группах, коллективно обсуждать определенный темами материал, а также инициировать самостоятельную работу студентов. При осмыслении содержания вопросов практических занятий преследуется цель соблюдать преемственность в профессиональном и в творческом развитии студентов.

Контроль самостоятельной работы студентов призван сделать процесс обучения более целостным и органичным. Его задача - не оставить без внимания даже, на первый взгляд, малозначительные вопросы.

Компьютерное тестирование позволяет осуществлять итоговый контроль знаний студентов. Тестовый материал включает в себя содержание вопросов по каждому из обозначенных программой разделов.

Каждый вопрос предполагает один или несколько вариантов ответов, среди которых имеются абсолютно неверный, правильный и/или в большей или меньшей степени раскрывающий сущность вопроса. В тестовых заданиях есть вопросы на соответствие. В процессе компьютерного тестирования, задача студента определяется как выбор правильного ответа из многообразия вариантов.

Вопросы и темы, отводимые на выполнение самостоятельной работы по дисциплине, а также критерии оценивания по каждому виду работы содержатся в разделе 8 РПД.

8. Оценочные средства для текущего контроля успеваемости, рубежной аттестации и промежуточной аттестации по итогам освоения дисциплины (ОК-12, ПК-20, ПК-28, ПК-29,ПК-32)

Рабочая программа предусматривает проведение лекционных и лабораторных занятий, а также следующие виды работ: самостоятельную работу студентов по подготовке устных ответов, обсуждений по темам дисциплины и решение задач.

Рабочая программа предполагает текущий, рубежный и промежуточный контроль знаний обучающихся.

Текущий контроль – это непрерывно осуществляемый мониторинг уровня освоения знаний и формирования умений и навыков в течение семестра. Текущий контроль знаний, умений и навыков студентов осуществляется в ходе учебных (аудиторных) занятий, проводимых по расписанию.

Формами текущего контроля могут быть опросы на лекционных и лабораторных занятиях, а также короткие (например, до 15 мин.) задания, выполняемые студентами в начале занятия с целью проверки наличия знаний, необходимых для усвоения нового материала или в конце занятия для выяснения степени усвоения материала.

Рубежный контроль осуществляется по окончании изучения части материала в заранее установленное время. Рубежный контроль проводится с целью определения качества

усвоения материала. В течение семестра проводится два таких контрольных мероприятия по графику.

Промежуточный контроль – итоговая оценка знаний студента, осуществляется по накопительной системе суммированием баллов, полученных в процессе текущего и рубежного контроля.

Форма промежуточного контроля – зачет.

Проведение текущего, рубежного и промежуточного контроля по дисциплине осуществляется в соответствии с Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования – программам бакалавриата, магистратуры и специалитета в СОГУ.

Балльная структура оценки

Форма контроля	**Макс. кол-во баллов**
Текущая оценка студента в течение 1-8 недели состоит из:	20
• Выполнения заданий на лабораторных занятиях	10
• Оценки самостоятельной работы	10
1-е рубежное тестирование	15
Текущая оценка студента в течение 9-16 недели состоит из:	20
• Выполнения заданий на лабораторных занятиях	10
• Оценки самостоятельной работы	10
2-е рубежное тестирование	15
Итого	**70**

Методика формирования результирующей оценки

В ходе текущего контроля студенты могут набрать 0-70 баллов:

1-я рубежная аттестация - максимально 35 баллов; из них:

- от 0 до 15 баллов (рубежная аттестация) – тестирование в центре тестирования СОГУ;
- от 0 до 20 баллов (текущая оценка) – активная работа за данный период на занятиях;

2-я рубежная аттестация – максимально 35 баллов; из них:

- от 0 до 15 баллов (рубежная аттестация) – тестирование в центре тестирования СОГУ;
- от 0 до 20 баллов (текущая оценка) – активная работа за данный период на занятиях.

Промежуточный контроль:

За устный ответ на зачете студент получает 0-30 баллов.

Студенты, получившие в ходе текущего и рубежного контроля 53-70 баллов, автоматически получают «Зачет».

Результирующая оценка складывается в соответствии с Положением о БРС оценивания обучающихся очной формы обучения по образовательным программам высшего образования – программам бакалавриата и специалитета в ФГБОУ ВО СОГУ.

8.1. Оценочные средства для текущего контроля успеваемости

Критерии оценивания самостоятельной работы обучающихся по дисциплине

Критерии оценки устного и/или письменного ответа на лабораторном занятии

Оценка	Критерий
5	Содержание ответа соответствует освещаемому вопросу, полностью раскрыта в ответе тема, ответ структурирован, даны правильные аргументированные ответы на уточняющие вопросы, демонстрируется высокий уровень участия в дискуссии.
4	Содержание ответа соответствует освещаемому вопросу, полностью раскрыта в ответе тема, даны правильные, аргументированные ответы на уточняющие вопросы, но имеются неточности, при этом ответ неструктурирован и демонстрируется средний уровень участия в дискуссии.
3	Содержание ответа соответствует освещаемому вопросу, но при полном раскрытии темы имеются неточности, даны правильные, но не аргументированные ответы на уточняющие вопросы, демонстрируется низкий уровень участия в дискуссии, ответ неструктурирован, информация трудна для восприятия.
2	Содержание ответа соответствует освещаемому вопросу, но при полном раскрытии темы имеются неточности, демонстрируется слабое владение категориальным аппаратом, даны правильные, но не аргументированные ответы на уточняющие вопросы, участие в дискуссии отсутствует, ответ неструктурирован, информация трудна для восприятия.

Примерные задачи по дисциплине

Задание 1:

Узнать:

1. Что обозначает термин "ресурсы"? Какие бывают ресурсы?
2. Что такое информационные ресурсы?

Рассмотреть:

1. Какие существуют подходы к понятию "информационные ресурсы"?

Доказать:

1. Всякий ресурс кроме информационного после использования исчезает.

Задание 2:

1. Разделиться на группы:
   Группа 1. Информационные опасности
   Группа 2. Классификация информационных угроз
   Группа 3. Компьютерные вирусы.
   Группа 4. Способы защиты информации
2. Используя ресурсы сети Интернет найти материал по своим заданиям,
3. выбрать самое главное
4. Весь собранный материал систематизировать и представить с помощью интеллект-карты.
5. Выбрать одного представителя от группы, который кратко подведет итог проведенной работы.

Задание 3:

Программы по юридическому статусу можно разделить на три большие группы: лицензионные, условно бесплатные и свободно распространяемые программы. Как можно охарактеризовать каждую группу? Заполните таблицу: запишите группу, к которой относится программа с предложенной характеристикой.

Характеристика программ	Группа

Версии программ с ограниченным сроком действия	
Новые недоработанные версии программных продуктов, распространяются с целью их широкого тестирования	
Устаревшие версии программ	
Версии программ с ограниченными возможностями	
Распространяются разработчиками на основании договоров с пользователями на платной основе	
Драйверы к новым устройствам или улучшенные драйверы к уже существующим драйверам	

Задание 4:
Используя шифр Цезаря, зашифруйте свои данные: Фамилию Имя Отчество.

Задание 5:
Выполните первый цикл алгоритма шифрования ГОСТ 28147 89 в режиме простой замены. Для получения 64 бит исходного текста используйте 8 первых букв из своих данных: Фамилии Имени Отчества.

Задание 6:
Сгенерируйте открытый и закрытый ключи в алгоритме шифрования RSA, выбрав простые числа p и q из первой сотни. Зашифруйте сообщение, состоящее из ваших инициалов: ФИО.

Задание 7:
Используя хеш-образ своей Фамилии, вычислите электронную цифровую подпись по схеме RSA.

8.2. Оценочные средства для проведения рубежной аттестации

Критерии оценивания результатов рубежного тестирования

Всего в тесте 15 вопросов. За каждый правильный ответ ставится 1 балл.

Примеры тестовых заданий для проведения рубежной аттестации

Какие проблемы таит в себе информационное общество?
Собственная безопасность
Защита прав личности
Безопасность государственных учреждений, защита от нападения
Защита интеллектуальной собственности

Какие внутренние информационные угрозы следует учесть при разработке мер информационной безопасности России?
Информационная война
Отставание по уровню информатизации
Преступная деятельность
Недостаточный уровень образования

К правовым методам, обеспечивающим информационную безопасность, относятся:
Разработка аппаратных средств обеспечения правовых данных

Разработка и установка во всех компьютерных правовых сетях журналов учета действий
Разработка и конкретизация правовых нормативных актов обеспечения безопасности

Основными источниками угроз информационной безопасности являются все указанное в списке:
Хищение жестких дисков, подключение к сети, инсайдерство
Перехват данных, хищение данных, изменение архитектуры системы
Хищение данных, подкуп системных администраторов, нарушение регламента работы

Виды информационной безопасности:
Персональная, корпоративная, государственная
Клиентская, серверная, сетевая
Локальная, глобальная, смешанная

Цели информационной безопасности – своевременное обнаружение, предупреждение:
несанкционированного доступа, воздействия в сети
инсайдерства в организации
чрезвычайных ситуаций

Основные объекты информационной безопасности:
Компьютерные сети, базы данных
Информационные системы, психологическое состояние пользователей
Бизнес-ориентированные, коммерческие системы

Основными рисками информационной безопасности являются:
Искажение, уменьшение объема, перекодировка информации
Техническое вмешательство, выведение из строя оборудования сети
Потеря, искажение, утечка информации

К основным принципам обеспечения информационной безопасности относится:
Экономической эффективности системы безопасности
Многоплатформенной реализации системы
Усиления защищенности всех звеньев системы

Основными субъектами информационной безопасности являются:
руководители, менеджеры, администраторы компаний
органы права, государства, бизнеса
сетевые базы данных, фаерволлы

8.3. Оценочные средства для проведения промежуточной аттестации

Критерии оценивания ответа студента на зачете

Характеристика ответа	Баллы
Дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний об объекте, проявляющаяся в свободном оперировании понятиями, умении выделить существенные и несущественные его признаки, причинно-следственные связи. Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ формулируется в терминах науки, изложен	46-50

литературным языком, логичен, доказателен, демонстрирует авторскую позицию студента.	
Дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний об объекте, доказательно раскрыты основные положения темы; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ изложен литературным языком в терминах науки. Могут быть допущены недочеты в определении понятий, исправленные студентом самостоятельно в процессе ответа.	41-45
Дан полный, развернутый ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи. Ответ четко структурирован, логичен, изложен в терминах науки. Однако допущены незначительные ошибки или недочеты, исправленные студентом с помощью «наводящих» вопросов преподавателя.	36-40
Дан полный, но недостаточно последовательный ответ на поставленный вопрос, но при этом показано умение выделить существенные и несущественные признаки и причинно-следственные связи. Ответ логичен и изложен в терминах науки. Могут быть допущены 1–2 ошибки в определении основных понятий, которые студент затрудняется исправить самостоятельно.	31-35
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.	26-30
Дан неполный ответ, логика и последовательность изложения имеют существенные нарушения. Допущены грубые ошибки при определении сущности раскрываемых понятий, теорий, явлений, вследствие непонимания студентом их существенных и несущественных признаков и связей. В ответе отсутствуют выводы. Умение раскрыть конкретные проявления обобщенных знаний не показано. Речевое оформление требует поправок, коррекции.	21-25
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.	1-20
Не получены ответы по базовым вопросам дисциплины.	0

Зачет проводится в устной форме.

Вопросы для подготовки к зачету

1. Понятие информации. Подходы к измерению информации
2. Кодирование текстовой информации

3. Кодирование графической информации
4. Информационно-техническая безопасность
5. Информационно-психологическая безопасность
6. Кодирование числовой информации
7. Теоретические вопросы организационного и правового обеспечения информационной безопасности
8. Методологические вопросы организационного и правового обеспечения информационной безопасности
9. Уголовная ответственность за посягательства на информационную безопасность
10. Информационная безопасность в предпринимательской деятельности
11. Банковская система Российской Федерации.
12. Концепция безопасности коммерческого банка
13. Единый подход к защите информации в финансовой сфере
14. Программное обеспечение для контроля подлинности документов.
15. Понятие информационной безопасности. Составляющие информационной безопасности.
16. Объекты, цели и задачи защиты информации.
17. Угрозы информационной безопасности: основные понятия. Виды и классификация угроз.
18. Основные угрозы целостности, конфиденциальности, доступности. Примеры.
19. Атака типа отказ в обслуживании.
20. Виды мер обеспечения информационной безопасности.
21. Программные средства защиты информации.
22. Административный уровень защиты информации: политика безопасности.
23. Разграничение прав пользователей в ОС Windows.
24. Защита ПК от несанкционированного доступа. Защита от несанкционированной загрузки ОС.
25. Идентификация и аутентификация: понятия, задачи. Аутентификация пользователей на основе паролей.
26. Идентификация и аутентификация: понятия, способы идентификации, Аутентификация пользователей по их биометрическим характеристикам.
27. Протоколирование и аудит: понятие, задачи, примеры.
28. Компьютерный вирус: понятие, пути проникновения. Классификация компьютерных вирусов.
29. Способы заражения программ. Признаки появления вирусов.
30. Защита от воздействия вирусов: понятие антивирусной программы. Классификация антивирусных программ.
31. Способы обнаружения вирусов.
32. Криптографические меры защиты информации: основные понятия, методы и алгоритмы шифрования.
33. Шифры перестановки и шифры замены.
34. Симметричные алгоритмы шифрования.
35. Ассиметричные алгоритмы шифрования. Алгоритм RSA.
36. Хэш-функции. Электронная цифровая подпись
37. Защита информации в сети.

38. Защита баз данных.
39. Закон об авторском праве.
40. Обзор российского законодательства в области защиты информации.
41. Федеральный закон «Об информации, информационных технологиях и о защите информации».

Показатели и критерии оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Уровень сформированности компетенций			
«Минимальный уровень не достигнут» (менее 50 баллов) Компетенции не сформированы. Знания отсутствуют, умения и навыки не сформированы.	«Минимальный уровень» (50-70 баллов) Компетенции сформированы. Сформированы базовые структуры знаний. Умения фрагментарны и носят репродуктивный характер. Демонстрируется низкий уровень самостоятельности практического навыка.	«Средний уровень» (71-85 баллов) Компетенции сформированы. Знания обширные, системные. Умения носят репродуктивный характер, применяются к решению типовых заданий. Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка.	«Высокий уровень» (86-100 баллов) Компетенции сформированы. Знания твердые, аргументированные, всесторонние. Умения успешно применяются к решению как типовых, так и нестандартных творческих заданий. Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка
Описание критериев оценивания			
Обучающийся демонстрирует: - существенные пробелы в знаниях учебного материала; - допускаются принципиальные ошибки при ответе на основные вопросы билета, отсутствует знание и понимание основных понятий и категорий; - непонимание сущности дополнительных вопросов в рамках заданий би-	Обучающийся демонстрирует: - знания теоретического материала; - неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; - неуверенные и неточные ответы на дополнительные вопросы; - недостаточное владение литературой, рекомендованной программой дисциплины; - умение без гру-	Обучающийся демонстрирует: - знание и понимание основных вопросов контролируемого объема программного материала; - твердые знания теоретического материала. -способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; - правильные и конкретные, без грубых ошибок, ответы на поставленные вопросы; - умение решать прак-	Обучающийся демонстрирует: - глубокие, всесторонние и аргументированные знания программного материала; - полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий в рамках обсуждаемых заданий; - способность устанавливать и объяснять связь практики и теории; - логически последовательные, содержательные, конкретные и исчерпывающие ответы

лета; - отсутствие умения выполнять практические задания, предусмотренные программой дисциплины; - отсутствие готовности (способности) к дискуссии и низкую степень контактности.	бых ошибок решать практические задания, которые следует выполнить.	тические задания, которые следует выполнить; - владение основной литературой, рекомендованной программой дисциплины; - наличие собственной обоснованной позиции по обсуждаемым вопросам. Возможны незначительные оговорки и неточности в раскрытии отдельных положений вопросов билета, присутствует неуверенность в ответах на	на все задания билета, а также дополнительные вопросы экзаменатора; - умение решать практические задания; - свободное использование в ответах на вопросы материалов рекомендованной основной и дополнительной литературы.
Оценка «незачтено»	*Оценка «зачтено»*	*Оценка «зачтено»*	*Оценка «зачтено»*

9. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2020. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450371 (дата обращения: 26.08.2020).

2. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449350 (дата обращения: 26.08.2020).

3. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2020. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/448295 (дата обращения: 26.08.2020).

4. Внуков, А. А. Защита информации в банковских системах : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2018. — 246 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01679-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/414083 (дата обращения: 26.08.2020).

5. Васильева, И. Н. Криптографические методы защиты информации : учебник и

практикум для академического бакалавриата / И. Н. Васильева. — Москва : Издательство Юрайт, 2019. — 349 с. — (Бакалавр. Академический курс). — ISBN 978-5-534-02883-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/433610 (дата обращения: 27.08.2020).

6. Трофимов, В. В. Информатика в 2 т. Том 1 : учебник для академического бакалавриата / В. В. Трофимов, М. И. Барабанова ; ответственный редактор В. В. Трофимов. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2019. — 553 с. — (Бакалавр. Академический курс). — ISBN 978-5-534-02613-9. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/434466 (дата обращения: 27.08.2020).

б) дополнительная литература:

1. Аверченков В.И. Организационная защита информации: учеб. пособие для вузов / В.И. Аверченков, М.Ю. Рытов. – Брянск: БГТУ, 2005. – 184 с.
2. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. — М.: Академический Проект; Гаудеамус, 2-е изд.— 2004. — 544 с.
3. Вострецова, Е.В. Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд-во Урал. ун-та, 2019.— 204 с.

в) *электронные библиотечные системы, с которыми у СОГУ имеется действующий договор, современные профессиональные базы, информационные справочные системы:*

- Информационно-правовой портал «Гарант» (http://www.garant.ru/).
- Справочная правовая система КонсультантПлюс (http://www.consultant.ru/).
- eLIBRARY.RU [Электронный ресурс]: научная электронная библиотека. – URL: http://www.elibrary.ru.
- Издательство «Юрайт» [Электронный ресурс]: электронно-библиотечная система. – URL: http://biblio-online.ru.
- Университетская библиотека online [Электронный ресурс]: электронно-библиотечная система. – URL: http://www.biblioclub.ru.
- ЭБС «Консультант студента» (https:// www.studmedlib.ru).
- Электронная база данных Правительства РФ «Электронное правительство» (https://www.google.com/url?q=https://rosstat.gov.ru).
- Курс «Кибербезопасность: что нужно знать о новом виде защиты?» (https://stepik.org/course/69690).
- Курс «Информационная безопасность: как защитить себя и свои аккаунты.» (https://stepik.org/course/68856/promo).
- Курс «Введение в кибербезопасность.» (https://stepik.org/course/61595/promo).

10. Материально-техническое оснащение дисциплины:

Проведение занятий лекционного типа предполагается в учебной аудитории факультета, в которой имеются: преподавательский стол; стул; столы обучающихся; стулья; кафедра; классная доска; мультимедийный комплекс (проектор, экран); ноутбук; колонки.

Проведение занятий семинарского типа предполагается в учебной аудитории факультета, в которой имеются: преподавательский стол; стул; столы обучающихся; стулья; ПК для обучающихся; классная доска, мультимедийный комплекс (проектор, экран), ноутбук, колонки. Эта же аудитория используется для выполнения групповых и индивидуальных консультаций, текущего контроля успеваемости.

Проведении рубежного тестирования предполагается в компьютерном классе №409 (учебный корпус №7 экономического факультета), в котором имеются: преподавательский стол, преподавательский стул, столы обучающихся, стулья, классная доска, мультимедийный комплекс (проектор, экран), колонки, ПК преподавателя, ПК для обучающихся.

Студенты имеют доступ к учебным и научным фондам библиотеки СОГУ, а также к электронным библиотечным ресурсам. Читальный зал библиотеки оснащен столами, стульями, ПК для обучающихся.

Состав лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

№ п/п	Наименование	№ договора (лицензия)
	Windows 7 Professional	№ 4100072800 Microsoft Products (MPSA) от 04.2016 г.
	Office Standard 2016	№ 4100072800 Microsoft Products (MPSA) от 04.2016 г.
	Антивирусное программное обеспечение Kasperksy Total Security	№17E0-180222-130819-587-185 от 26.02.2018 до 14.03.2019 г.
	Программа для ЭВМ «Банк вопросов для контроля знаний»	Разработка СОГУ Свидетельство о государственной регистрации программы для ЭВМ №2015611829 от 06.02.2015 г. (бессрочно)
	Система тестирования Sunrav WEB Class	№468 от 03.12.2013 ИП Сунгатулин Р.Т.(бессрочно)
	КонсультантПлюс	№430-2017/614 от11.01.2017 г. ООО «Фаст-Информ» (бессрочно)
	Гарант	№01/20 от 17.01.2020 действителен до 31.12.2020 ООО Регион-15