МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
И.о. заведующего кафедрой
математического анализа
Шабров С.А.

01.07.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.О.33 Информационная безопасность

Код и наименование дисциплины в соответствии с учебным планом

1.Код и наименование программы:

02.03.01 Математика и компьютерные науки

2. Профиль: Математические методы и компьютерные технологии в естествознании, экономике и управлении, Математическое и компьютерное моделирование

3. Квалификация (степень) выпускника: Бакалавр

4. Форма обучения: Очная

5. Кафедра, отвечающая за реализацию дисциплины: Кафедра математического анализа

6. Составители программы:
(ФИО, ученая степень, ученое звание)
Шабров Сергей Александрович, доктор физ-мат. наук, доцент

7. Рекомендована: Научно-методическим Советом математического факультета, протокол №0500-07 от 29.06.2021

8. Учебный год: 2024-2025 **Семестр(ы):** 8

9 .Цели и задачи учебной дисциплины:

Целями освоения учебной дисциплины являются:

- предоставление обучаемым знаний основных типов и способов защиты информации; приобретение студентами умения проектировать системы защиты информации;

Задачи учебной дисциплины:

овладение современными программными и аппаратными средствами защиты информации**.**

10. Место учебной дисциплины в структуре ООП:

Дисциплина относится к математическому и естественнонаучному циклу ФГОС ВО в структуре ООП бакавриата. Для изучения дисциплины слушатели должны владеть базовыми знаниями школьного курса «Информатика» в области алгоритмизации и программирования. Приобретенные в результате обучения знания, умения и навыки используются во всех без исключения математических и естественнонаучных дисциплинах, модулях и практиках. Полученные знания могут быть использованы при продолжении образования в магистратуре и в дальнейшей трудовой деятельности выпускников.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ОПК-5	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий, в том числе отечественного производителя, и с учетом основных требований информационной безопасности	ОПК-5.1	ОПК-5.1 Знает основные положения и концепции прикладного и системного программирования, архитектуры компьютеров и сетей (в том числе и глобальных), современные языки программирования, технологии создания и эксплуатации программных продуктов и программных комплексов	Знать: основные понятия информационной безопасности; основные направления защиты информации; законодательство Российской Федерации в области защиты информации; современные методы и средства защиты информации в информационно-телекоммуникационных системах; архитектуру защищённых экономических систем. Уметь: разрабатывать политику информационной безопасности; проводить оценку угроз безопасности объекта информатизации; реализовывать простые информационные технологии реализующие методы защиты информации; применять методики оценки уязвимости в информационно-телекоммуникационных сетях; проектировать системы защиты информации. Владеть: методами защиты информации; средствами защиты информации в сетях ЭВМ.
		ОПК-5.2	ОПК-5.2 Умеет использовать их в профессиональной	Знать: основные понятия информационной безопасности; основные направления защиты информации; законодательство

			деятельности.	Российской Федерации в области защиты информации; современные методы и средства защиты информации в информационно-телекоммуникационных системах; архитектуру защищённых экономических систем. Уметь: разрабатывать политику информационной безопасности; проводить оценку угроз безопасности объекта информатизации; реализовывать простые информационные технологии реализующие методы защиты информации; применять методики оценки уязвимости в информационно-телекоммуникационных сетях; проектировать системы защиты информации. Владеть: методами защиты информации; средствами защиты информации в сетях ЭВМ.
		ОПК-5.3.	ОПК-5.3. Имеет практические навыки разработки ПО	Знать: основные понятия информационной безопасности; основные направления защиты информации; законодательство Российской Федерации в области защиты информации; современные методы и средства защиты информации в информационно-телекоммуникационных системах; архитектуру защищённых экономических систем. Уметь: разрабатывать политику информационной безопасности; проводить оценку угроз безопасности объекта информатизации; реализовывать простые информационные технологии реализующие методы защиты информации; применять методики оценки уязвимости в информационно-телекоммуникационных сетях; проектировать системы защиты информации. Владеть: методами защиты информации; средствами защиты информации в сетях ЭВМ.
ОПК-4	Способен находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем	ОПК-4.1	ОПК-4.1 Знает базовые основы современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности	Знать: основные понятия информационной безопасности; основные направления защиты информации; законодательство Российской Федерации в области защиты информации; современные методы и средства защиты информации в информационно-телекоммуникационных системах; архитектуру защищённых экономических систем. Уметь: разрабатывать политику информационной безопасности; проводить оценку угроз безопасности объекта информатизации; реализовывать простые информационные технологии реализующие методы защиты информации; применять методики оценки уязвимости в информационно-телекоммуникационных сетях; проектировать системы защиты

				информации. Владеть: методами защиты информации; средствами защиты информации в сетях ЭВМ.
		ОПК-4.2	ОПК-4.2 Умеет использовать этот математический аппарат в профессиональной деятельности	Знать: основные понятия информационной безопасности; основные направления защиты информации; законодательство Российской Федерации в области защиты информации; современные методы и средства защиты информации в информационно-телекоммуникационных системах; архитектуру защищённых экономических систем. Уметь: разрабатывать политику информационной безопасности; проводить оценку угроз безопасности объекта информатизации; реализовывать простые информационные технологии реализующие методы защиты информации; применять методики оценки уязвимости в информационно-телекоммуникационных сетях; проектировать системы защиты информации. Владеть: методами защиты информации; средствами защиты информации в сетях ЭВМ.
		ОПК-4.3.	ОПК-4.3. Имеет практический опыт применения современного математического аппарата, связанного с проектированием, разработкой, реализацией и оценкой качества программных продуктов и программных комплексов в различных областях человеческой деятельности	Знать: основные понятия информационной безопасности; основные направления защиты информации; законодательство Российской Федерации в области защиты информации; современные методы и средства защиты информации в информационно-телекоммуникационных системах; архитектуру защищённых экономических систем. Уметь: разрабатывать политику информационной безопасности; проводить оценку угроз безопасности объекта информатизации; реализовывать простые информационные технологии реализующие методы защиты информации; применять методики оценки уязвимости в информационно-телекоммуникационных сетях; проектировать системы защиты информации. Владеть: методами защиты информации; средствами защиты информации в сетях ЭВМ.

12. Объем дисциплины в зачетных единицах/час.(*в соответствии с учебным планом)* **2**/72

Форма промежуточной аттестации*(зачет/экзамен) зачет*

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость	
		Всего	По семестрам
			8 семестр
Контактная работа		20	20
в том числе:	лекции	10	10
	практические	10	10
	лабораторные	-	-
	курсовая работа	-	-
	контроль	-	-
Самостоятельная работа		52	52
Итого:		**72**	**72**

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1. Лекции		
1.1	Общие вопросы информационной безопасности	Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации. Международные стандарты информационного обмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.
1.2	Государственная система информационной безопасности	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Доктрина информационной безопасности Российской Федерации. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
1.3	Угрозы безопасности	Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Виды угроз. Основные нарушения. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.
1.4	Теоретические основы	Основные положения теории информационной

	методов защиты информационных систем	безопасности информационных систем. Модели безопасности и их применение. Формальные модели безопасности. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant. Мандатная модель Белла-ЛаПадулы. Ролевая политика безопасности. Ограничения на области применения формальных моделей.
1.5	Методы защиты средств вычислительной техники	Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от НСД. Средства операционной системы. Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности.
2. Практические занятия		
2.1	Общие вопросы информационной безопасности	Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене. Защита информации, тайна, средства защиты информации. Международные стандарты информационного обмена. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.
2.2	Государственная система информационной безопасности	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Доктрина информационной безопасности Российской Федерации. Структура государственной системы информационной безопасности. Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
2.3	Угрозы безопасности	Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Виды угроз. Основные нарушения. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.
2.4	Теоретические основы методов защиты информационных систем	Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение. Формальные модели безопасности. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа.

		Модель распространения прав доступа Take-Grant. Мандатная модель Белла-ЛаПадулы. Ролевая политика безопасности. Ограничения на области применения формальных моделей.
2.5	Методы защиты средств вычислительной техники	Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от НСД. Средства операционной системы. Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)					
		Лекции	Практические	Лабораторные	Самостоятельная работа	Контроль	Всего
1	Общие вопросы информационной безопасности	2	2	0	10	0	14
2	Государственная система информационной безопасности	2	2	0	10	0	14
3	Угрозы безопасности	2	2	0	10	0	14
4	Теоретические основы методов защиты информационных систем	2	2	0	10	0	14
5	Методы защиты средств вычислительной техники	2	2	0	12	0	16
	Итого:	10	10	0	52	0	72

14. Методические указания для обучающихся по освоению дисциплины

(рекомендации обучающимся по освоению дисциплины: работа с конспектами лекций, презентационным материалом, выполнение практических заданий, тестов, заданий текущей аттестации и т.д.)

Для обеспечения систематической и регулярной работы по изучению дисциплины и успешного прохождения аттестаций студентам рекомендуется придерживаться следующего порядка обучения:

1. Самостоятельно определить объем времени, необходимого для проработки каждой темы.
2. Регулярно изучать каждую тему дисциплины как по конспектам лекции, так и по рекомендованной литературе, используя различные формы индивидуальной работы.
3. Согласовывать с преподавателем виды работы по изучению дисциплины.
4. По завершении отдельных тем передавать выполненные работы (домашние задания) преподавателю.

5. При успешном прохождении рубежных контрольных испытаний студент может претендовать на сокращение программы промежуточной (итоговой) аттестации по дисциплине.

Методические указания для обучающихся при самостоятельной работе.

1. Самостоятельная работа обучающихся направлена на самостоятельное освоение всех тем и вопросов учебной дисциплины, предусмотренных программой. Самостоятельная работа является обязательным видом деятельности для каждого обучающегося, ее объем по учебному курсу определяется учебным планом. При самостоятельной работе обучающийся взаимодействует с рекомендованными материалами при минимальном участии преподавателя.
2. Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и ресурсами сети Internet является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся заинтересованное отношение к конкретной проблеме.
3. Вопросы, которые вызывают у обучающихся затруднения при подготовке, должны быть заранее сформулированы и озвучены во время занятий в аудитории для дополнительного разъяснения преподавателем.
4. Для успешного и плодотворного обеспечения итогов самостоятельной работы разработаны учебно-методические указания к самостоятельной работе студентов над различными разделами дисциплины.
5. Виды самостоятельной работы: конспектирование учебной и научной литературы; проработка учебного материала (по конспектам лекций, учебной и научной литературе); работа в электронной библиотечной системе; работа с информационными справочными системами, выполнение домашних заданий (практических и теоретических); выполнение контрольных работ; подготовка к практическим занятиям; работа с вопросами для самопроверки.
6. Все задания, выполняемые студентами самостоятельно, подлежат последующей проверке преподавателем.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины *(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)*

а) основная литература:

№ п/п	Источник
1	Голуб, Владимир Александрович. Информационная безопасность СМИ: криптографическая защита информации : учебное пособие / В.А. Голуб ; Воронеж. гос. ун-т, Фак. журналистики .— Воронеж : Факультет журналистики ВГУ, 2010 .— 99 с.

б) дополнительная литература:

№ п/п	*Источник*
2	Мещеряков Р. В. Информационная безопасность: Учеб. пособие – Томск.: Изд-во Том. политехн. Ун-т, 2004 – 168 с.
3	Мещеряков Р. В., Шелупанов А. А. Специальные вопросы информационной безопасности. – Томск.: Изд-во ИОА ТНЦ СО РАН, 2003 – 250 с.
4	Мещеряков Р. В., Шелупанов А. А., Белов Е. Б., Лось В. П. Основы информационной безопасности. – М.: Горячая линия – Телеком, 2006. – 540 с.
5	Герасименко В. А. Защита информации в автоматизированных системах

	обработки данных. В 2-х кн. – М.: Энергоатомиздат, 1994.
6	Герасименко В. А., Малюк А. А. Основы защиты информации. – М.: «Инкомбук», 1997. – 540 с.

в)информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Ресурс
13.	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/)

* Вначале указываются ЭБС, с которыми имеются договора у ВГУ, затем открытые электронно-образовательные ресурсы

16. Перечень учебно-методического обеспечения для самостоятельной работы *(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)*

№ п/п	Источник
1	Мещеряков Р. В. Информационная безопасность: Учеб. пособие – Томск.: Изд-во Том. политехн. Ун-т, 2004 – 168 с.
2	Мещеряков Р. В., Шелупанов А. А. Специальные вопросы информационной безопасности. – Томск.: Изд-во ИОА ТНЦ СО РАН, 2003 – 250 с.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

Урок-лекция с применением современных технологий (урок-презентация).

18. Материально-техническое обеспечение дисциплины:

1. Типовое оборудование учебной аудитории.
2. Зональная научная библиотека, электронный каталог Научной библиотеки ВГУ (http://www.lib.vsu.ru

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Общие вопросы информационной безопасности	ОПК-4 ОПК-5	ОПК – 4.1, ОПК – 4.2, ОПК – 4.3, ОПК – 4.1, ОПК – 4.2, ОПК – 4.3	Промежуточная аттестация – зачет, письменная работа, контрольно-измерительные материалы к зачету.
2	Государственная система информационной безопасности	ОПК-4 ОПК-5	ОПК – 4.1, ОПК – 4.2, ОПК – 4.3, ОПК – 4.1, ОПК – 4.2, ОПК – 4.3	Промежуточная аттестация – зачет, письменная работа, контрольно-измерительные материалы к зачету.

3	Угрозы безопасности	ОПК-4 ОПК-5	ОПК – 4.1, ОПК – 4.2, ОПК – 4.3, ОПК – 4.1, ОПК – 4.2, ОПК – 4.3	Промежуточная аттестация – зачет, письменная работа, контрольно-измерительные материалы к зачету.
4	Теоретические основы методов защиты информационных систем	ОПК-4 ОПК-5	ОПК – 4.1, ОПК – 4.2, ОПК – 4.3, ОПК – 4.1, ОПК – 4.2, ОПК – 4.3	Промежуточная аттестация – зачет, письменная работа, контрольно-измерительные материалы к зачету.
5	Методы защиты средств вычислительной техники	ОПК-4 ОПК-5	ОПК – 4.1, ОПК – 4.2, ОПК – 4.3, ОПК – 4.1, ОПК – 4.2, ОПК – 4.3	Промежуточная аттестация – зачет, письменная работа, контрольно-измерительные материалы к зачету.
Промежуточная аттестация Форма контроля - зачет				Перечень вопросов к зачету.

Перечень вопросов к зачету:

1. Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность.
2. Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене.
3. Защита информации, тайна, средства защиты информации. Международные стандарты информационного обмена.
4. Показатели информации: важность, полнота, адекватность, релевантность, толерантность. Требования к защите информации.
5. Комплексность системы защиты информации: инструментальная, структурная, функциональная, временная.
6. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
7. Доктрина информационной безопасности Российской Федерации. Структура государственной системы информационной безопасности.
8. Структура законодательной базы по вопросам информационной безопасности. Лицензирование и сертификация в области защиты информации.
9. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
10. Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Виды угроз. Основные нарушения.
11. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз.
12. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.
13. Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение.

14. Формальные модели безопасности. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant. Мандатная модель Белла-ЛаПадулы.
15. Ролевая политика безопасности. Ограничения на области применения формальных моделей.
16. Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от НСД. Средства операционной системы.
17. Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности.

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств: письменная работа

Примерный комплект заданий для письменных работ

Вариант 1.

1. Основные понятия и определения. Понятия информация, информатизация, информационная система, информационная безопасность.
2. Основные положения теории информационной безопасности информационных систем. Модели безопасности и их применение.

Составитель _____ С.А. Шабров
(подпись)

27.05.2019

Вариант 2.

1.Понятия автора и собственника информации, взаимодействие субъектов в информационном обмене.
2.Ролевая политика безопасности. Ограничения на области применения формальных моделей.

Составитель _____ С.А. Шабров
(подпись)

27.05.2019

Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на занятиях.

К основным формам текущего контроля можно отнести устный опрос, проверку домашних заданий, контрольные работы.

Задание для текущего контроля и проведения промежуточной аттестации должны быть направлены *на оценивание:*

1. уровня освоения теоретических и практических понятий, научных основ профессиональной деятельности;

2. степени готовности обучающегося применять теоретические и практические знания и профессионально значимую информацию, сформированности когнитивных умений.

3. приобретенных умений, профессионально значимых для профессиональной деятельности.

Текущий контроль предназначен для проверки хода и качества формирования компетенций, стимулирования учебной работы обучаемых и совершенствования методики освоения новых знаний. Он обеспечивается проведением контрольных заданий и домашних работ, проверкой конспектов лекций, периодическим опросом слушателей на занятиях.

Формы, методы и периодичность текущего контроля определяет преподаватель.

При текущем контроле уровень освоения учебной дисциплины и степень сформированности компетенции определяются оценками «зачтено» и «не зачтено».

Описание технологии проведения

Тестирование и контрольные работы проводятся письменно.

Требование к выполнению заданий

Письменная работа

За письменную работу ставится оценка «зачтено», в случае, если обучающийся выполнил:

- правильно в полном объеме все задания письменной работы, показал отличные владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного материала;

- обучающийся выполнил все задания с небольшими неточностями и показал хорошие владения навыками применения полученных знаний и умений при решении профессиональных задач в рамках усвоенного материала;

- обучающий выполнил половину из предложенных заданий правильно, остальные с существенными неточностями и показал удовлетворительное владение навыками полученных знаний и умений при решении профессиональных задач в рамках усвоенного материала.

В остальных случаях обучающемуся ставится за письменную работу «не зачтено».

20.2 Промежуточная аттестация

Промежуточная аттестация предназначена для определения уровня освоения всего объема учебной дисциплины. Промежуточная аттестация по дисциплине «Информационная безопасность» проводится в форме зачета.

Промежуточная аттестация, как правило, осуществляется в конце семестра и завершает изучение дисциплины. Промежуточная аттестация помогает оценить более крупные совокупности знаний и умений, в некоторых случаях – даже формирование определенных профессиональных компетенций. На зачете оценивается уровень освоения учебной дисциплины и степень сформированности компетенции определяются оценками «зачтено», «не зачтено».

Описание технологии проведения

На зачете студент вытягивает билет, который содержит один теоретический вопрос и один практический. Все вопросы и задачи, входящие в билеты, охватывают весь материал, изучаемый за весь семестр.

Примерный комплект билетов для зачета

Контрольно-измерительный материал № 1

1. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
2. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз.

Составитель _____ С.А. Шабров
(подпись)

27.05.2019

Контрольно-измерительный материал № 2

1. Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Виды угроз. Основные нарушения.
2. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.

Составитель _____ С.А. Шабров
(подпись)

27.05.2019

Критерии выставления оценок:

Оценки	Критерии
Зачтено	обучающийся показывает свой интеллектуальный и общекультурный уровень, знает предмет учебной дисциплины, логично излагает изученный материал, умеет применять теоретические знания для решения практических заданий.
Не зачтено	обучающийся демонстрирует фрагментарные знания и умения или отсутствие их.