Подвальный
Евгений Семенович
Подписано цифровой подписью: Подвальный Евгений Семенович
Дата: 2025.03.25 14:20:30 +03'00'

Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Воронежский филиал РАНХиГС

Факультет управления, экономики и права

Кафедра естественно-научных и социальных дисциплин

УТВЕРЖДЕНА
Решением кафедры
естественно-научных и социальных дисциплин
Протокол от «05» марта 2024 г. № 7

ПРОГРАММА БАКАЛАВРИАТА

Организационный менеджмент

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ, реализуемой без применения электронного (онлайн) курса

Б1.В.ДВ.08.02 «Основы информационной безопасности»

38.03.02 «Менеджмент»

Форма обучения – очная

Год набора – 2023

Воронеж, 2024 г.

Автор-составитель:
Профессор, доктор технических наук, заведующий кафедрой естественно-научных и социальных дисциплин Подвальный Евгений Семенович

Заведующий кафедрой Естественно-научных и социальных дисциплин
профессор, доктор технических наук Подвальный Евгений Семенович

РПД «Основы информационной безопасности» одобрена на заседании кафедры Естественно-научных и социальных дисциплин. Протокол от «05» марта 2024 г. № 7

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы 4
2. Объем и место дисциплины в структуре образовательной программы 5
3. Содержание и структура дисциплины 6
4. Материалы текущего контроля успеваемости обучающихся 9
5. Оценочные материалы промежуточной аттестации по дисциплине 11
6. Методические указания для обучающихся по освоению дисциплины 17
7. Учебная литература и ресурсы информационно-телекоммуникационной сети "Интернет", учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине 14
7.1. Основная литература 15
7.2. Дополнительная литература 16
7.3. Нормативные правовые документы 16
7.5. Интернет-ресурсы 16
7.6. Иные источники 16
8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы 16

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

1.1 Дисциплина Б1.В.ДВ.08.02 «Основы информационной безопасности» обеспечивает овладение следующей компетенцией с учетом этапа:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
ПКс- 10	Способен применять в профессиональной деятельности основные требования информационно-коммуникационной безопасности в делопроизводстве организации, при подготовке и оформлении организационно-распорядительных документов	ПКс – 10.1.2	Способен применять методы и соблюдать требования информационно-коммуникационной безопасности при решении задач профессиональной деятельности

1.2. В результате освоения дисциплины у студентов должны быть:

ОТФ/ТФ *(при наличии профстандарта)*/ трудовые или профессиональные действия	Код этапа освоения компетенции	Результаты обучения
ПКс- 10 направлена на формирование трудовых функций, связанных с основами безопасной работы с компьютерной техникой и информационно-коммуникационными сетями в целях защиты информации	ПКс – 10.1.2	на уровне знаний: - место информационной безопасности в системе национальной безопасности страны; - угрозы информационной безопасности государства; - содержание информационной войны, методы и средства ее ведения; - виды информации ограниченного доступа, в соответствии с требованиями Российского законодательства; - основные понятия в области информационной безопасности и методологические принципы создания систем защиты информации; - методы и средства и обеспечения информационной безопасности компьютерных систем, механизмы защиты информации; - критерии оценки защищенности автоматизированных систем и современные методы обеспечения их информационной безопасности; - особенности обеспечения информационной безопасности автоматизированных систем при обработке информации, составляющей государственную тайну;
		на уровне умений: - выбирать и анализировать показатели

		качества и критерии оценки систем и отдельных методов и средств защиты информации; - подбирать информацию для решения задач защиты информации.
		на уровне навыков: - навыками активной состязательной деятельности в условиях информационного противоборства; - навыками подбора нормативных и методических материалов по вопросам обеспечения информационной безопасности.

2. Объем и место дисциплины в структуре ОП ВО

Дисциплина Б1.В.ДВ.08.02 «Основы информационной безопасности» относится к дисциплинам по выбору ОП ВО направления 38.03.02 «Менеджмент». Освоение дисциплины на очной форме обучения осуществляется во втором семестре 1 курса. Общая трудоемкость дисциплины 2 ЗЕ, что составляет 72 академических часа, лекции – 14 часов, практические занятия – 16 часов, самостоятельная работа – 42 часов.

Освоение дисциплины «Основы информационной безопасности» опирается на результаты освоения дисциплины «Цифровые технологии в менеджменте»:

знания в области об информационной, цифровой и библиографической культуре; о правилах взаимодействия с участниками информационных процессов при обмене информацией (документами, файлами, сообщениями); об информационной безопасности на различных уровнях (государственном, корпоративном, личном); о современных цифровых технологиях и примерах их применения в менеджменте и бизнесе; о роли и месте баз данных в информационной системе организации;

умения соблюдать требования информационной безопасности при работе с информационными системами; организации рабочей электронной среды, обеспечивающей надежную и безопасную работу с информацией (сообщениями, файлами, программами)

Данная дисциплина может быть реализована с применением дистанционных образовательных технологий (ДОТ). Доступ к системе дистанционных образовательных осуществляется каждым обучающимся самостоятельно с любого устройства на портале: https://lms.ranepa.ru. Пароль и логин к личному кабинету / профилю предоставляется студенту в деканате.

Все формы текущего контроля, проводимые в системе дистанционного обучения, оцениваются в системе дистанционного обучения. Доступ к видео и материалам лекций предоставляется в течение всего семестра. Доступ к каждому виду работ и количество попыток на выполнение задания предоставляется на ограниченное время согласно регламенту дисциплины, опубликованному в СДО. Преподаватель оценивает выполненные обучающимся работы не позднее 10 рабочих дней после окончания срока выполнения.

Общее количество академических часов или астрономических часов, выделенных на контактную работу с преподавателем представлено в Таблице 1:

Таблица 1.1

Вид учебных занятий и самостоятельная работа		**Объем дисциплины, акад.час.**							
		Всего (акад.час.)	**Семестр**						
			1	2	3	4	5	6	7	8
Очная форма обучения										
Контактная работа обучающихся с преподавателем, в том числе:		**30**		**30**						
лекционного типа (Л)		**14**		**14**						
практического (семинарского) типа (ПЗ)		**16**		**16**						
Самостоятельная работа обучающихся (СР)		**42**		**42**						
Промежуточная аттестация	***форма***	**зачет**		**зачет**						
	час									
Общая трудоемкость (акад. час. / з.е.)		**72/2**		**72/2**						

3. Содержание и структура дисциплины

Таблица 2.1

Очная форма обучения

0	Наименование тем (разделов)	Объем дисциплины, акад.час.						Форма текущего контроля успеваемости**, промежуточной аттестации***
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СРО	
			Л/ ДОТ	ЛР/ ДОТ	ПЗ/ ДОТ	КСР		
Тема 1	Национальная безопасность Российской Федерации	8	2/0	0/0	2/0	0	4	О, П
Тема 2	Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере							
Тема 3	Основные понятия и общеметодологические принципы теории информационной безопасности.	6	0/0	0/0	0/0	0	6	
Тема 4	Понятие и виды защищаемой информации.	4	0/0		2/0	0	2	П
Тема 5	Понятие и виды угроз информационной безопасности.	8	2/0	0/0	2/0	0	4	О, П
Тема 6	Информационная безопасность и информационное противоборство.							
Тема 7	Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны.	8	0/0	0/0	2/0	0	6	П

Тема 8	Методы и средства обеспечения информационной безопасности компьютерных систем	6	2/0	0/0	0/0	0	4	О
Тема 9	Механизмы защиты информации в автоматизированных системах	8	2/0	0/0	2/1,5	0	4	О, П
Тема 10	Формальные модели безопасности автоматизированных систем	8	2/0	0/0	2/0	0	4	О, П
Тема 11	Методы и критерии оценки защищенности компьютерных систем	8	2/0	0/0	2/0	0	4	О, П
Тема 12	Защита информации, обрабатываемой в автоматизированных системах от технических разведок	8	2/0	0/0	2/0	0	4	О, П
Промежуточная аттестация								Зач
Всего:		**72/2**	**14**	**0**	**16**	**0**	**42**	

Примечание
*** – формы текущего контроля успеваемости: опрос (О), презентация (П).*
**** - формы промежуточной аттестации: зачет (Зач).*

Содержание дисциплины

Модуль 1. Информационная безопасность в системе национальной безопасности

Тема 1. Национальная безопасность Российской Федерации.

Понятие национальной безопасности. Виды безопасности и сферы жизнедеятельности личности, общества и государства. Национальные интересы РФ и стратегические национальные приоритеты. Цели и смысл государственной службы. Роль специалиста по защите информационной безопасности в обеспечении национальной безопасности государства.

Тема 2. Основы государственной политики и угрозы безопасности Российской Федерации в информационной сфере.

Основные составляющие национальных интересов Российской Федерации в информационной сфере. Информационная безопасность Российской Федерации. Интересы личности в информационной сфере. Интересы общества в информационной сфере. Интересы государства в информационной сфере. Виды угроз информационной безопасности Российской Федерации. Источники угроз информационной безопасности Российской Федерации. Внешние источники угроз. Внутренние источники угроз. Направления обеспечения информационной безопасности государства. Проблемы региональной информационной безопасности.

Тема 3. Основные понятия и общеметодологические принципы теории информационной безопасности.

Источники понятий в области информационной безопасности. Основные понятия информационной безопасности: документированная информация, безопасность информации, конфиденциальность, целостность, доступность информации, защита информации, система

защиты информации. Общеметодологические принципы теории информационной безопасности.

Тема 4. Понятие и виды защищаемой информации.

Понятие и сущность защищаемой информации. Права и обязанности обладателя информации. Виды защищаемой информации: государственная тайна, служебная тайна, профессиональная тайна, коммерческая тайна, персональные данные. Перечень сведений конфиденциального характера. Понятие интеллектуальной собственности и особенности ее защиты.

Модуль 2. Информационная война, методы и средства ее ведения

Тема 5. Понятие и виды угроз информационной безопасности.

Понятие угрозы информационной безопасности. Фактор, воздействующий на защищаемую информацию. Типы дестабилизирующих факторов. Классификация и виды угроз информационной безопасности. Внутренние и внешние источники угроз информационной безопасности. Угрозы утечки информации и угрозы несанкционированного доступа. Основные элементы канала реализации угрозы безопасности информации.

Тема 6. Информационная безопасность и информационное противоборство.

Субъекты информационного противоборства. Цели информационного противоборства. Составные части и методы информационного противоборства. Информационное оружие, его классификация и возможности.

Тема 7. Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны.

Методы нарушения конфиденциальности, целостности и доступности информации. Причины, виды, каналы утечки и искажения информации. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны. Компьютерная система как объект информационной войны.

Модуль 3. Обеспечение информационной безопасности компьютерных систем

Тема 8. Методы и средства обеспечения информационной безопасности компьютерных систем.

Компьютерная система как объект информационной безопасности. Общая характеристика способов и средств защиты информации. Правовая, техническая, криптографическая, физическая защита информации. Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности. Программно-аппаратные средства обеспечения информационной безопасности.

Тема 9. Механизмы защиты информации в автоматизированных системах.

Содержание сервисов безопасности программно-технического уровня. Идентификация и аутентификация, управление доступом и авторизация, протоколирование и аудит. Криптография для сервисов безопасности: шифрование и контроль целостности. Экранирование. Анализ защищенности. Обеспечение доступности. Туннелирование. Управление.

Тема 10. Формальные модели безопасности автоматизированных систем.

Назначение формальных моделей безопасности. Политика безопасности. Монитор безопасности обращений. Дискреционная и мандатная модели безопасности. Формальные модели управления доступом. Модель Харрисона-Руззо-Ульмана. Модель Белла-ЛаПадулы. Формальные модели целостности. Модель Кларка-Вилсона. Модель Биба. Совместное использование моделей безопасности. Ролевое управление доступом.

Тема 11. Методы и критерии оценки защищенности компьютерных систем.

Модели, стратегии и системы обеспечения информационной безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Критерии безопасности компьютерных систем «Оранжевая книга». Общие критериит безопасности информационных технологий. Руководящие документы Гостехкомиссии (ФСТЭК) России. Стандарты по управлению информационной безопасностью ISO/IEC 27000.

Тема 12. Защита информации, обрабатываемой в автоматизированных системах от технических разведок.

Классификация и возможности технических разведок. Компьютерная разведка. Технические каналы утечки информации при эксплуатации автоматизированных систем. Электромагнитное воздействие и эффекты его воздействия. Защита автоматизированных систем и средств вычислительной техники от внешнего электромагнитного воздействия.

4. Материалы текущего контроля успеваемости обучающихся

4.1. В ходе реализации дисциплины Б1.В.ДВ.08.02 «Основы информационной безопасности» используются следующие методы текущего контроля успеваемости обучающихся:

- *при проведении занятий лекционного типа:* опрос.
- *при проведении занятий семинарского типа:* презентации студентов по заданным темам с последующим групповым обсуждением.
- *при контроле результатов самостоятельной работы студентов:* контроль осуществляется на занятиях семинарского типа.

4.2. Материалы текущего контроля успеваемости обучающихся.

Типовые оценочные материалы по модулю 1:

Темы для выполнения презентаций по модулю:

1. Место и роль информационной безопасности в различных сферах жизнедеятельности личности (общества, государства).
2. Национальная безопасность. Сущность и виды безопасности.
3. Информационная безопасность в системе национальной безопасности РФ.
4. Влияние процессов информатизации общества на составляющие информационной безопасности.
5. Состав и содержание направлений информационной безопасности.
6. Правовая база обеспечения информационной безопасности личности (общества, государства).
7. Государственная информационная политика. История, становление, сущность и содержание, основные направления.
8. Виды информации с точки зрения информационной безопасности.
9. Виды защищаемой информации.
10. Интересы личности (общества, государства) в информационной сфере.
11. Проблемы региональной информационной безопасности.
12. Основные нормативно-правовые акты в области информационной безопасности.
13. Исторические этапы развития системы защиты информации в России.
14. Экономические факторы обеспечения безопасности коммерческой организации.

Вопросы для проведения устного опроса:

1. Понятие национальной безопасности Российской Федерации.
2. Национальные интересы РФ и стратегические национальные приоритеты.
3. Роль информационной безопасности в обеспечении национальной безопасности государства.
4. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
5. Понятие информационной безопасности Российской Федерации.
6. Интересы личности общества и государства в информационной сфере.
7. Перечислите виды угроз информационной безопасности Российской Федерации.

8. Назовите внешние и внутренние источники угроз информационной безопасности Российской Федерации.
9. Методы обеспечения информационной безопасности Российской Федерации.
10. Назовите общеметодологические принципы теории информационной безопасности.
11. Понятие и сущность защищаемой информации.
12. Права и обязанности обладателя информации.
13. Виды защищаемой информации.
14. Перечень сведений конфиденциального характера.
15. Понятие интеллектуальной собственности и особенности ее защиты.

Типовые оценочные материалы по модулю 2:

Темы для выполнения презентаций по модулю:

1. Угрозы информационной безопасности и факторы, воздействующие на информацию.
2. Причины, виды, каналы утечки и искажение информации.
3. Информационное оружие, его классификация и возможности.
4. Информационное противоборство.
5. Методы нарушения конфиденциальности (целостности, доступности) информации.
6. Национальные интересы РФ и угрозы национальной безопасности.
7. Угрозы информационной безопасности Российской Федерации.
8. Анализ угроз информационной безопасности компьютерных систем.
9. Внешние (внутренние) источники угроз информационной безопасности государства.
10. Актуальные проблемы безопасности компьютерных систем.
11. Актуальные проблемы информационной безопасности при использовании мобильных средств связи.
12. Актуальные проблемы информационной безопасности в социальных сетях.
13. Актуальные проблемы информационной безопасности критически важных объектов.
14. Компьютерная система как объект информационного воздействия.

Вопросы для проведения устного опроса:

1. Какой фактор, воздействует на защищаемую информацию. Назовите типы дестабилизирующих факторов.
2. Классификация и виды угроз информационной безопасности.
3. Угрозы утечки информации и угрозы несанкционированного доступа.
4. Основные элементы канала реализации угрозы безопасности информации.
5. Субъекты и цели информационного противоборства.
6. Составные части и методы информационного противоборства.
7. Информационное оружие, его классификация и возможности.
8. Методы нарушения конфиденциальности, целостности и доступности информации.
9. Что такое информационная война и как она воздействует на информационные системы.
10. Обеспечение безопасности объектов информационной сферы государства в информационной войне.

Типовые оценочные материалы по модулю 3:

Темы для выполнения презентаций по модулю:

1. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.
2. Современные методы и средства защиты информации.
3. Задачи подготовки специалистов по защите информации.
4. Отечественные и зарубежные стандарты в области информационной безопасности.
5. Правовые основы защиты персональных данных.
6. Криптология и основные этапы ее становления и развития.
7. Комплексный подход к обеспечению информационной безопасности.
8. Основные механизмы и сервисы защиты информации.
9. Правовое обеспечение информационной безопасности.
10. Инженерно-техническое обеспечение информационной безопасности.
11. Организация физической защиты информации.
12. Организация работы с персоналом в системе информационной безопасности.
13. Политика информационной безопасности предприятия и организации.

14. Правовые (организационно-технические, экономические) методы обеспечения информационной безопасности.
15. Обеспечение информационной безопасности компьютерных систем.
16. Анализ современных подходов к построению систем защиты информации.
17. Критерии оценки защищенности компьютерных систем, методы и средства обеспечения их информационной безопасности.
18. Особенности обеспечения информационной безопасности компьютерных систем при обработке информации, составляющей государственную тайну.
19. Обеспечение безопасности технических систем и человека в условиях использования информационного оружия.
20. Анализ факторов, определяющих безопасность технических систем.
21. Классификация и возможности технических разведок.
22. Показатели защищенности средств вычислительной техники от НСД к информации.
23. Пароль как средство защиты от НСД.
24. Требования по защите информации в автоматизированных системах от НСД.
25. Оценка безопасности информационных технологий по общим критериям.

Вопросы для проведения устного опроса:
1. Перечислите основные способы защиты информации.
2. Понятие и классификация средств защиты информации.
3. Характеристика средств защиты информации.
4. Уровни информационной безопасности и их характеристика.
5. Сервисы безопасности программно-технического уровня.
6. Идентификация и аутентификация как сервисы безопасности.
7. Управление доступом и его виды.
8. Авторизация как сервис безопасности.
9. Протоколирование и аудит как сервисы безопасности.
10. Криптографические сервисы безопасности.
11. Какие бывают сервисы безопасности, охарактеризуйте.
12. Назначение формальных моделей безопасности. Политика безопасности.
13. Дискреционная модель безопасности. Модель Харрисона-Руззо-Ульмана.
14. Мандатная модель безопасности. Модель Белла-ЛаПадулы.
15. Формальные модели целостности.
16. Понятие ролевого управления доступом.
17. Модели, стратегии и системы обеспечения информационной безопасности.
18. Назовите критерии безопасности компьютерных систем ≪Оранжевая книга≫.
19. Общие критерии безопасности информационных технологий.
20. Критерии и классы защищенности СВТ, и АС. Руководящие документы ФСТЭК России.
21. Стандарты по управлению информационной безопасностью ISO/IEC 27000.
22. Классификация и возможности технических разведок.
23. Что такое компьютерная разведка.
24. Технические каналы утечки информации при эксплуатации автоматизированных систем.
25. Электромагнитное воздействие и эффекты его воздействия.

5. Оценочные материалы промежуточной аттестации по дисциплине.
5.1 Зачет проводится с применением следующих методов (средств):
Зачет на очной форме обучения проводится в форме подведения итогов по результатам выполнений заданий текущего контроля успеваемости и выполнения тестовых заданий.
При проведении зачета с использованием дистанционных образовательных технологий промежуточная аттестация проводится, в форме тестирования.

5.2. Оценочные материалы промежуточной аттестации

Этап освоения компетенции	Промежуточный/ ключевой индикатор оценивания	Критерий оценивания

Этап освоения компетенции	Промежуточный/ ключевой индикатор оценивания	Критерий оценивания
ПКс – 10.1.2 Способен применять методы и соблюдать требования информационно-коммуникационной безопасности при решении задач профессиональной деятельности	Собрана полная информация. Исключена недостоверная информация.	Самостоятельно осуществляет поиск информации в глобальной сети Интернет, базах данных

Типовые оценочные средства

Оценочным средством промежуточной аттестации на очной форме обучения является накопительная оценка результатов выполнения текущего контроля по дисциплине и выполнения тестовых заданий.

Шкала и процедура оценивания определены Регламентом Воронежского филиала РАНХиГС «Порядок применения балльно-рейтинговой системы оценки знаний обучающихся в Воронежском филиале РАНХиГС, утвержденным приказом от 08 февраля 2018 года № 114-35.

Начисление баллов при изучении дисциплины

Таблица 7

Виды контактной работы обучающихся с преподавателем	**Баллы**
Посещение лекционных занятий	2
Посещение практических занятий	1
Результаты занятий:	
-ответы на вопросы устного опроса	1
-выполнение заданий практических занятий по теме 1-5	2
-выполнение заданий практических занятий по теме 6	3,5
Диапазон оценивания результатов тестирования 4,7 до 5,00 3,8 до 4,69 3,00 до 3,79 0 до 2,99	 40-34 34-28 28-21 20 и менее

Схема перевода набранных обучающимся баллов в пятибалльную систему

Сумма баллов, набранных студентом по дисциплине за все виды работ, переводится в традиционные оценки. В зависимости от суммы набранных баллов студенту в пересчете на традиционную шкалу оценок выставляются:
- 0-50 баллов - «не зачтено»;
- 51-100 - «зачтено».

Тестовые задания по дисциплине «Основы информационной безопасности»

1. Программа, которая может размножаться, присоединяя свой код к другой программе, называется:
Выберите один ответ.
a. Компилятор
b. Интернет-черви
c. Вирус

2. Величиной (размером) ущерба (вреда), ожидаемого в результате несанкционированного доступа к информации или нарушения доступности информационной системы, называется:
Выберите один ответ.
a. Воздействием (влиянием)
b. Потерей
c. Силой

3. Код, способный самостоятельно, то есть без внедрения в другие программы, вызвать распространение своих копий по информационной системе и их выполнение, называется:
Выберите один ответ.
a. Троянской программой
b. Червем
c. Вирусом

4. Уровень риска, который считается доступным для достижения желаемого результата, называется:
Выберите один ответ.
a. Устойчивостью
b. Терпимостью по отношению к риску
c. Независимостью

5. Компьютер с одним процессором в каждый конкретный момент времени может выполнять команд:
Выберите один ответ.
a. Две
b. Одну
c. Сколько зададут

6. Алгоритмы реального времени, заранее назначающие каждому процессу фиксированный приоритет, после чего выполняющие приоритетное планирование с переключениями, называются:
Выберите один ответ.
a. Статическими алгоритмами
b. Алгоритмы RMS
c. Динамическими алгоритмами

7. Системные файлы, обеспечивающие поддержку структур файловой системы, называются:
Выберите один ответ.
a. Каталоги
b. Символьные файлы
c. Регулярные файлы

8. Коды, обладающие способностью к распространению (возможно, с изменениями) путем внедрения в другие программы, называются:
Выберите один ответ.
a. Вирусами
b. Руткитами
c. Червями

9. Требованием к информационной системе, являющимся следствием действующего законодательства, миссии и потребностей организации, называется:
Выберите один ответ.
a. Правилами безопасности
b. Требованием безопасности
c. Мерами безопасности

10. Процессом идентификации рисков применительно к безопасности информационной системы, определения вероятности их осуществления и потенциального воздействия, а также дополнительный контрмер, ослабляющий (уменьшающий) это воздействие, называется:
Выберите один ответ.
a. Управление риском
b. Предупреждением рисков
c. Анализом рисков

11. Компьютерная система, в которой два или более центральных процессоров делят полный доступ к общей оперативной памяти, называется:
Выберите один ответ.
a. Мультипроцессоры типа «хозяин-подчиненный»
b. Симметричный мультипроцессор
c. Мультипроцессор с общей памятью

Ключ к тесту:

1	2	3	4	5	6
c	a	b	b	b	a
7	8	9	10	11	
a	a	b	a	b	

В программе используется следующая шкала оценок:
1. За каждый ответ на вопрос студент может получить от 0 до 1 балла. Для получения 1 балла студент должен отметить только все правильные ответы.
2. Оценка за ответ рассчитывается по формуле:

Оценка = КВП/ОКП/(КВН + 1), где

- КВП – количество выбранных правильных ответов;
- ОКП – общее количество правильных вариантов в вопросе;
- КВН – количество выбранных неправильных вариантов.

Шкала оценивания

Система оценивания	**Диапазон оценивания**
Отлично (оценка пять)	от 4,7 до 5,00
Хорошо (оценка четыре)	3,8 до 4,69
Удовлетворительно (оценка три)	3,00 до 3,79
Неудовлетворительно (оценка два)	0 до 2,99

Методические материалы

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующих этапы формирования компетенций определены порядком «Порядок проведения текущего контроля успеваемости обучающихся по образовательным программам высшего образования – программам бакалавриата, программам магистратуры в Воронежском филиале РАНХиГС», утвержденным приказом от 08 февраля 2018 года № 114-39 и порядком «Порядок проведения промежуточной аттестации обучающихся по образовательным программам высшего образования - программам бакалавриата, программам магистратуры в Воронежском филиале РАНХиГС», утвержденным приказом от 08 февраля 2018 года № 114-40.

6. Методические указания для обучающихся по освоению дисциплины

Для качественного выполнения презентации необходимо выполнить следующие требования:

1. Презентация должна содержать введение (термины и определения, актуальность, цели, задачи), основной раздел, раскрывающий данную тему, который должен содержать описание конкретного примера системы и процесса ее управления, заключение.

2. Соответствие целей поставленной теме.
3. Язык изложения материала должен быть понятен аудитории.
4. Актуальность, точность и полезность содержания.
5. Использование качественной достоверной информации.
6. Тематическая последовательность.
7. Графическая информация (иллюстрации, графики, таблицы, диаграммы и т.д.)
8. Работа с дополнительными источниками.

Выделим наиболее общие требования к средствам, формам и способам представления материала в электронной презентации:

1. Сжатость и краткость изложения, максимальная информативность текста.
2. Объединение семантически связанных информационных элементов в целостно воспринимающиеся группы.
3. Каждому положению (каждой идее) должен быть отведен отдельный абзац текста.
4. Основная идея абзаца должна находиться в самом начале (в первой строке абзаца). Это связано с тем, что лучше всего запоминаются первая и последняя мысли абзаца.
5. При проектировании характера и последовательности предъявления учебного материала должен соблюдаться принцип стадийности: информация может разделяться в пространстве (одновременное отображение в разных зонах одного слайда) или во времени (размещение информации на последовательно демонстрируемых слайдах).
6. Вся вербальная информация должна тщательно проверяться на отсутствие орфографических, грамматических и стилистических ошибок.
7. Графика должна органично дополнять текст.

Специальные требования к презентации:

1. Объём презентации не менее 25 слайдов.
2. Наличие примеров использования комплексной интегрированной системы информационных ресурсов в практической деятельности.
3. Защита презентации.

Советы для успешного показа презентационной работы:

- Не перегружайте свою презентацию оптическими и акустическими эффектами. Мерцающие буквы, быстро сменяющиеся страницы, постоянно крутящиеся на экране объекты и непрерывно звучащая музыка могут раздражать и отвлекать слушателей.
- Не перегружайте и сами слайды. Наглядность и хорошая обозримость только облегчат слушателям понимание происходящего.
- Попросите коллегу помочь в перелистывании слайдов. Дайте ему текст доклада с указанием номеров слайдов, чтобы он мог ориентироваться по этому документу, когда перелистывать слайды. Отрепетируйте с ним доклад заранее. Не следует включать функцию автоматического переключения слайдов.

7. Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет», включая перечень учебно-методического обеспечения дисциплины

7.1. Основная литература

1. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495525

2. Суворова, Г. М. Информационная безопасность: учебное пособие для вузов / Г. М. Суворова. — Москва: Издательство Юрайт, 2020. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496741

3. Зенков, А. В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. — Москва: Издательство Юрайт, 2020. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497002

7.2. Дополнительная литература

1. Герасименко В. А. и др. Основы защиты информации М.: Изд-во МИФИ, 1997–537 с.

2. Цирлов В.Л. Основы информационной безопасности: краткий курс. Ростов-на-Дону: Феникс, 2008.— 254 с.

3. Расторгуев СП. Информационная война М. : Радио и связь, 1999 .—415 с.

4. Данилов А.Н., Полшков А.В., Шабуров А.С. Информационная безопасность Пермь: ПГТУ, 2004.-150 с.

5. Ярочкин В. И. Информационная безопасность: учебник для вузов, 5-е изд. - М: Акад. проект, 2008–543 с.

7.3. Нормативно-правовые документы

1. Положение об организации самостоятельной работы студентов федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации» (в ред. Приказа РАНХиГС от 11.05.2016 г. № 01-2211).

2. Регламент Воронежского филиала РАНХиГС «Порядок применения балльно-рейтинговой системы оценки знаний обучающихся в Воронежском филиале РАНХиГС, утвержденный приказом от 08 февраля 2018 года № 114-35.

3. Стратегия национальной безопасности Российской Федерации доь2020 года.

7.4. Интернет-ресурсы

1. http://www.biblioclub.ru «Университетская библиотека онлайн»
2. Куб — электронная библиотека http://www.koob.ru/
3. http://www.pedlib.ru/
4. http://www.klex.ru/11m
5. http://window.edu.ru/window/catalog
6. Сервер компании НИП "Информзащита" - http://www.infosec.ru/
7. Информационный бюллетень "Jet Info" с тематическим разделом по информационной безопасности http://www.jetinfo.ru/
8. Федеральный портал «Российское образование www.edu.ru
9. Российский биометрический портал www.biometrics.ru

7.5. Иные источники

1. Издательство «Открытые системы» [Сайт]. - URL: http://www.osp.ru.
2. Научная электронная библиотека eLIBRARY.RU. - URL:http://elibrary.ru/.
3. Электронно-библиотечная система Издательства «Лань» - URL: http://e.lanbook.com/
4. Электронно-библиотечная система «Университетская библиотека online» - URL: http://old.biblioclub.ru/.
5. Электронно-библиотечная система «ЮРАЙТ» - URL: http://www.biblio-online.ru/)
6. Электронно-библиотечная система «IPRbooks» - URL: http://www. iprbookshop.ru/.
7. Электронно-библиотечная система «ZNANIUM.COM» - URL: http://www.znanium.com (издательство ИНФРА-М).

8. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Для материально-технического обеспечения дисциплины используются: аудиторный фонд; компьютерный класс с возможностью доступа к глобальной сети Интернет, специализированная аудитория с ПК и мультимедийным проектором; библиотечно-информационные ресурсы.

В учебном процессе используются следующие лицензионные программные продукты: Microsoft office 2007, Windows xp, Касперский, Справочная правовая система «Консультант Плюс», Справочная правовая система «Гарант».