

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Воронежский государственный технический университет»


УТВЕРЖДАЮ
Декан ФИТКБ
/Гусев П.Ю./
31.08.2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

**«Стандартизация и методология управления информационными
рисками»**

**Направление подготовки 10.06.01 ИНФОРМАЦИОННАЯ
БЕЗОПАСНОСТЬ**

**Профиль 05.13.19 Методы и системы защиты информации,
информационная безопасность**

Квалификация выпускника Исследователь. Преподаватель-исследователь

Нормативный период обучения 4 года

Форма обучения очная

Год начала подготовки 2021

Автор программы

Заведующий кафедрой Систем информационной безопасности



К.А. Разинкин



А.Г. Остапенко

Руководитель ОПОП



А.Г. Остапенко

Воронеж 2021

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины: приобретение знаний, умений и навыков принятия решений в области анализа рисков в управлении информационной безопасностью

1.2. Задачи освоения дисциплины

изучение зарубежных и национальных стандартов и фреймворков риск-менеджмента в сфере информационной безопасности
исследование методологий риск-менеджмента и инструментальных средств анализа и управления рисками

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Стандартизация и методология управления информационными рисками» относится к дисциплинам вариативной части блока Б1.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Стандартизация и методология управления информационными рисками» направлен на формирование следующих компетенций:

ОПК-3 - способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности

ПК-4 - способность пользоваться стандартами и владение методами управления информационными рисками

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ОПК-3	знать основные положения зарубежных и национальных стандартов и фреймворков риск-менеджмента в сфере информационной безопасности
	уметь применять стандарты ИБ для построения единой системы менеджмента ИБ организации
ПК-4	знать методологии управления информационными рисками
	уметь осуществлять формализацию математического аппарата управления информационными рисками
	владеть инструментальными средствами для управления рисками

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Стандартизация и методология управления информационными рисками» составляет 4 з.е.

**Распределение трудоемкости дисциплины по видам занятий
очная форма обучения**

Виды учебной работы	Всего часов	Семестры
		4
Аудиторные занятия (всего)	36	36
В том числе:		
Лекции	36	36
Самостоятельная работа	108	108
Виды промежуточной аттестации - зачет с оценкой	+	+
Общая трудоемкость: академические часы зач.ед.	144 4	144 4

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц ц	СРС	Всего, час
1	Зарубежные стандарты, и фреймворки риск-менеджмента в сфере информационной безопасности	BS 7799-1:2005 — Британский стандарт BS 7799 первая часть. BS 7799 Part 1 — Code of Practice for Information Security Management (Практические правила управления информационной безопасностью) описывает 127 механизмов контроля, необходимых для построения системы управления информационной безопасностью (СУИБ) организации, определённых на основе лучших примеров мирового опыта (best practices) в данной области. Этот документ служит практическим руководством по созданию СУИБ BS 7799-2:2005 — Британский стандарт BS 7799 вторая часть стандарта. BS 7799 Part 2 — Information Security management — specification for information security management systems (Спецификация системы управления информационной безопасностью) определяет спецификацию СУИБ. Вторая часть стандарта используется в качестве критериев при проведении	6	18	24

		официальной процедуры сертификации СУИБ организации. BS 7799-3:2006 — Британский стандарт BS 7799 третья часть стандарта. Новый стандарт в области управления рисками информационной безопасности Фреймворк "NIST Risk Management Framework". Стандарт NIST SP 800-39 "Managing Information Security Risk". Стандарт NIST SP 800-37 "Risk Management Framework for Information Systems and Organizations". Стандарт NIST SP 800-30 "Guide for Conducting Risk Assessments". Стандарт NIST SP 800-137 "Information Security Continuous Monitoring" . Стандарт ISO/IEC 27005:2018 "Information technology - Security techniques - Information security risk management". Стандарт ISO/IEC 27102:2019 "Information security management - Guidelines for cyber-insurance"			
2	Методологи и риск-менеджмента	Методология FRAP. Методология OCTAVE. Методология FMEA. Методология CRAMM. Методология FAIR . Методология Microsoft. Концепция CSO ERM	6	18	24
3	Национальные стандарты Российской Федерации в области защиты информации	ГОСТ Р ИСО/МЭК 27004-2011 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения ГОСТ Р ИСО/МЭК 27004-2011 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. Information technology. Security techniques. Information security management. Measurement. Дата введения в действие 01.01.2012. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Information technology. Security techniques. Information security risk management. Дата введения в дей-	6	18	24

		<p>ствие 01.12.2011. ГОСТ Р ИСО/МЭК 31010-2011 Менеджмент риска. Методы оценки риска ГОСТ Р ИСО/МЭК 31010-2011 Менеджмент риска. Методы оценки риска (Risk management. Risk assessment methods). Дата введения в действие: 01.12.2012 ГОСТ Р ИСО 31000-2010 Менеджмент риска. Принципы и руководство</p>			
4	Оценка рисков информационной безопасности	<p>Идентификация активов: описание бизнес-процессов Идентификация требований безопасности: реестр требований безопасности; требования законодательства и нормативной базы контрактные обязательства, требования бизнеса Определение ценности активов: критерии оценки ущерба; таблица ценности активов; особенности интервьюирования бизнес-пользователей Определение приоритетов аварийного восстановления Анализ угроз и уязвимостей: профиль и жизненный цикл угрозы; описание угроз безопасности; классификации угроз уязвимости информационной безопасности; идентификация организационных уязвимостей; идентификация технических уязвимостей; оценка угроз и уязвимостей Определение величины риска: калибровка шкалы оценки риска; пример оценки риска отчет об оценке рисков</p>	6	18	24
5	Обработка рисков информационной безопасности	<p>Процесс обработки рисков. Способы обработки риска: принятие риска. уменьшение риска. передача риска. избежание риска Оценка возврата инвестиций в информационную безопасность Принятие решения по обработке риска План обработки рисков Декларация о применимости механизмов контроля Профили рисков информационной безопасности</p>	6	18	24
6	Инструментальные средства для управления	<p>Выбор инструментария для оценки рисков Общие недостатки и ограничения коммерческих программных продуктов</p>	6	18	24

	рисками	Обзор методов и инструментальных средств управления рисками			
			Итого	36	108
					144

5.2 Перечень лабораторных работ

Не предусмотрено учебным планом

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе: «аттестован»; «не аттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ОПК-3	знать основные положения зарубежных и национальных стандартов и фреймворков риск-менеджмента в сфере информационной безопасности	знание основные положения зарубежных и национальных стандартов и фреймворков риск-менеджмента в сфере информационной безопасности	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь применять стандарты ИБ для построения единой системы менеджмента ИБ организации	умение применять стандарты ИБ для построения единой системы менеджмента ИБ организации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-4	знать методологии управления информационными рисками	знание методологии управления информационными рисками	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь осуществлять формализацию математического аппарата управления информационными рисками	умение осуществлять формализацию математического аппарата управления информационными рисками	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	владеть инструментальными средствами для управления рисками	владение инструментальными средствами для управления рисками	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
--	---	--	---	---

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 4 семестре для очной формы обучения по четырехбалльной системе:

«отлично»; «хорошо»; «удовлетворительно»; «неудовлетворительно».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Отлично	Хорошо	Удовл.	Неудовл.
ОПК-3	знать основные положения зарубежных и национальных стандартов и фреймворков риск-менеджмента в сфере информационной безопасности	Тест	Выполнение теста на 90-100%	Выполнение теста на 80- 90%	Выполнение теста на 70- 80%	В тесте менее 70% правильных ответов
	уметь применять стандарты ИБ для построения единой системы менеджмента ИБ организации	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
ПК-4	знать методологии управления информационными рисками	Тест	Выполнение теста на 90-100%	Выполнение теста на 80- 90%	Выполнение теста на 70- 80%	В тесте менее 70% правильных ответов
	уметь осуществлять формализацию математического аппарата управления информационными рисками	Решение стандартных практических задач	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены
	владеть инструментальными средствами для управления рисками	Решение прикладных задач в конкретной предметной области	Задачи решены в полном объеме и получены верные ответы	Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах	Продемонстрирован верный ход решения в большинстве задач	Задачи не решены

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1. Согласно закону "О техническом регулировании", стандарт - это документ, в котором в целях добровольного многократного использования сформулированы характеристики продукции требование соблюдения единообразия технических и иных характеристик

изделие, характеристики которого считаются эталонными

2. Для передаваемых данных протокол передачи записей обеспечивает **конфиденциальность**

целостность

доступность

3. В число основных понятий обобщенного прикладного программного интерфейса службы безопасности входят:

сервис безопасности

механизм безопасности

контекст безопасности

4. Обычно политика безопасности запрещает:

разделять счета пользователей

заводить новые счета пользователей

ликвидировать счета пользователей

5. Согласно спецификации Internet-сообщества "Как реагировать на нарушения информационной безопасности", под нарушением информационной безопасности понимается:

потеря конфиденциальности информации

нарушение целостности информации

несанкционированное копирование информации

6. В стандарте BS 7799 фигурируют следующие группы регуляторов безопасности:

политика безопасности

программа безопасности

общеорганизационные аспекты защиты

7. В стандарте FIPS 140-2 фигурируют следующие группы требований безопасности:

конечноавтоматная модель

формальная модель политики безопасности

поведенческая модель

8. В соответствии с курсом, к числу важнейших видов общих функциональных требований к сервисам безопасности принадлежат:

идентификация (FIA_UID)

аутентификация (FIA_UAU)

выявление и реагирование на неудачи аутентификации (FIA_AFL)

9.Версия 2.1 "Общих критериев" содержит

10 классов функциональных требований безопасности

11 классов функциональных требований безопасности

12 классов функциональных требований безопасности

10.Произвольное (дискреционное) управление доступом основывается

на

атрибутах безопасности (FDP_ACF.1)

иерархических атрибутах безопасности (FDP_IFF.2)

управлении информационными потоками (FDP_IFC.1)

7.2.2 Примерный перечень заданий для решения стандартных задач

1. Согласно стандарту ГОСТ Р ИСО/МЭК 27001-2006 установление контекста это ...

определение основных критериев, необходимых для менеджмента риска ИБ, определение области применения и границ, а также создание соответствующей организационной структуры, занимающейся менеджментом риска ИБ

оценивание уровня классификации информационного актива, на который оказывается влияние;

оценка степени нарушения ИБ (например, утрата конфиденциальности, целостности и доступности);

2. Критериями оценки рисков информационной безопасности обычно являются

финансовые и иные последствия, связанные с событиями нарушения ИБ

утрата конфиденциальности, целостности и доступности

степень ущерба или величины расходов, понесенных организацией вследствие события, связанного с ИБ

3. Критерии влияния разрабатываются и определяются исходя из

Ответ: ... степени ущерба или величины расходов, понесенных организацией вследствие события, связанного с ИБ

4. Критерии влияния разрабатываются и определяются с учетом:

Ответ: уровня классификации информационного актива, на который оказывается влияние; нарушения ИБ (например, утрата конфиденциальности, целостности и доступности); нарушения оперативной деятельности (как собственной, так и третьих сторон); потери ценности бизнеса и финансовой ценности; нарушения планов и конечных сроков; ущерба для репутации; нарушения законодательных, нормативных или договорных требований.

4. Критерии принятия риска зависят от

политик, намерений, целей организации и интересов причастных сторон.

финансовых и иных последствий, связанные с событиями нарушения ИБ

области применения и границ, а также создание соответствующей организационной структуры, занимающейся менеджментом риска ИБ

5. Идентификация риска (risk identification) –

процесс нахождения, составления перечня и описания элементов риска формализация финансовых и иных последствий, связанные с событиями нарушения ИБ

задание области применения и границ, а также создание соответствующей организационной структуры, занимающейся менеджментом риска ИБ

6. Какие этапы реализации большинства угроз безопасности (жизненный цикл угроз), НЕ включают в себя следующие процессы:

зарождение;

развитие;

проникновение в АС;

проникновение в критичную информацию;

инициализация;

результат действия;

регенерация.

выбор способа реализации

7. Какой вариант не относится к обработке риска:

снижение риска,

сохранение риска,

предотвращение риска

перенос риска

ликвидация риска

8. Снижение риска это -....

действия, предпринятые для уменьшения вероятности, негативных последствий или того и другого вместе, связанных с риском

принятие бремени потерь или выгод от конкретного риска

задание границ применения менеджмента риска, а также создание соответствующей организационной структуры, занимающейся менеджментом риска ИБ

9. Предотвращение риска это -....

решение не быть вовлеченным в рискованную ситуацию или действие, предупреждающее вовлечение в нее.

разделение с другой стороной бремени потерь или выгод от риска

принятие бремени потерь или выгод от конкретного риска

10. Критерии принятия риска устанавливаются на этапе...

анализа контекста

оценивания риска

коммуникации риска

11. В стандарте NIST 800-30:2002 рассматриваются вопро-

Ответ: интеграции управления риском в жизненный цикл развития системы

7.2.3 Примерный перечень заданий для решения прикладных задач

Для обеспечения безопасности удаленного взаимодействия с корпоративной сетью было предложено 5 альтернатив. Для выбора наиболее подходящего решения эксперты оценивали альтернативы по двум критериям: стоимости внедрения и сопровождения (K_1) и предполагаемой эффективности (K_2). Необходимо выбрать лучшее решение, используя различные принципы (идеальности, оптимальности, лексикографический, главного критерия, максимина, равенства, абсолютной и относительной уступки), если:

Весы критериев одинаковы;

Второй критерий в два раза важнее первого.

Вариант 1

K_1	Эксперты									
Альтернативы	\mathcal{E}_1	\mathcal{E}_2	\mathcal{E}_3	\mathcal{E}_4	\mathcal{E}_5	\mathcal{E}_6	\mathcal{E}_7	\mathcal{E}_8	\mathcal{E}_9	\mathcal{E}_{10}
A_1	4	4	3	3	2	5	3	4	3	3
A_2	4	5	6	7	5	4	5	5	6	4
A_3	7	7	8	8	6	8	7	7	6	6
A_4	2	1	3	3	3	2	2	1	4	3
A_5	4	5	5	6	4	6	5	6	5	4

K_2	Эксперты									
Альтернативы	\mathcal{E}_1	\mathcal{E}_2	\mathcal{E}_3	\mathcal{E}_4	\mathcal{E}_5	\mathcal{E}_6	\mathcal{E}_7	\mathcal{E}_8	\mathcal{E}_9	\mathcal{E}_{10}
A_1	4	2	2	3	4	2	1	3	2	3
A_2	6	5	5	4	6	7	5	7	6	6
A_3	6	8	8	9	7	8	8	8	7	8
A_4	6	7	6	6	7	5	6	7	7	5
A_5	3	5	3	3	4	5	4	3	5	4

Вариант 2

K_1	Эксперты									
Альтернативы	\mathcal{E}_1	\mathcal{E}_2	\mathcal{E}_3	\mathcal{E}_4	\mathcal{E}_5	\mathcal{E}_6	\mathcal{E}_7	\mathcal{E}_8	\mathcal{E}_9	\mathcal{E}_{10}
A_1	6	7	3	2	3	6	4	5	4	2

A ₂	4	2	6	6	6	5	6	6	5	3
A ₃	9	6	8	7	7	7	6	7	8	6
A ₄	5	4	3	4	4	3	3	2	3	4
A ₅	6	3	5	7	5	7	4	7	4	5

K ₂	Эксперты									
Альтернативы	Э ₁	Э ₂	Э ₃	Э ₄	Э ₅	Э ₆	Э ₇	Э ₈	Э ₉	Э ₁₀
A ₁	5	3	1	4	5	1	2	2	3	4
A ₂	4	6	4	5	7	6	6	6	5	6
A ₃	5	9	7	8	8	7	7	7	6	7
A ₄	7	8	5	5	9	4	7	6	6	6
A ₅	4	6	2	4	5	4	5	2	4	5

Вариант 3

K ₁	Эксперты									
Альтернативы	Э ₁	Э ₂	Э ₃	Э ₄	Э ₅	Э ₆	Э ₇	Э ₈	Э ₉	Э ₁₀
A ₁	4	4	3	3	2	5	3	4	3	3
A ₂	4	5	6	7	5	4	5	5	6	4
A ₃	7	7	8	8	6	8	7	7	6	6
A ₄	2	1	3	3	3	2	2	1	4	3
A ₅	4	5	5	6	4	6	5	6	5	4

K ₂	Эксперты									
Альтернативы	Э ₁	Э ₂	Э ₃	Э ₄	Э ₅	Э ₆	Э ₇	Э ₈	Э ₉	Э ₁₀
A ₁	4	2	2	3	4	2	1	3	2	3
A ₂	6	5	5	4	6	7	5	7	6	6
A ₃	6	8	8	9	7	8	8	8	7	8
A ₄	6	7	6	6	7	5	6	7	7	5
A ₅	3	5	3	3	4	5	4	3	5	4

Альтернативы	Э ₁	Э ₂	Э ₃	Э ₄	Э ₅	Э ₆	Э ₇	Э ₈	Э ₉	Э ₁₀
A ₁	6	8	7	5	8	9	7	5	6	6
A ₂	2	3	2	1	2	3	6	5	4	5
A ₃	8	9	8	7	4	5	8	6	9	8
5A ₄	4	4	5	6	6	5	4	5	5	6
A ₅	3	2	1	4	5	6	2	3	2	1

Вариант 6

K ₁	Эксперты									
Альтернативы	Э ₁	Э ₂	Э ₃	Э ₄	Э ₅	Э ₆	Э ₇	Э ₈	Э ₉	Э ₁₀
A ₁	3	2	1	2	3	2	5	3	2	1
A ₂	6	5	4	5	6	5	4	5	6	5
A ₃	6	7	8	9	6	5	7	8	9	5
7A ₄	3	6	9	5	4	8	2	6	9	8
A ₅	9	2	5	6	8	6	4	3	8	3

K ₂	Эксперты									
Альтернативы	Э ₁	Э ₂	Э ₃	Э ₄	Э ₅	Э ₆	Э ₇	Э ₈	Э ₉	Э ₁₀
A ₁	9	8	7	4	5	6	8	4	5	8
A ₂	6	5	6	5	4	5	5	6	6	4
A ₃	5	7	6	6	8	8	9	7	6	9
A ₄	3	4	5	2	3	4	5	6	6	7
A ₅	5	6	4	5	6	5	4	5	6	4

Вариант 7

K ₁	Эксперты									
Альтернативы	Э ₁	Э ₂	Э ₃	Э ₄	Э ₅	Э ₆	Э ₇	Э ₈	Э ₉	Э ₁₀
A ₁	6	9	8	7	8	5	6	9	8	8
A ₂	4	5	5	3	6	5	4	6	4	5

A ₃	3	2	1	2	1	1	2	2	1	1
A ₄	4	4	4	4	4	4	4	4	4	4
A ₅	6	9	8	7	5	8	8	9	8	9

K ₂	Эксперты									
Альтернативы	Э ₁	Э ₂	Э ₃	Э ₄	Э ₅	Э ₆	Э ₇	Э ₈	Э ₉	Э ₁₀
A ₁	9	8	7	5	6	7	9	8	7	8
A ₂	6	5	5	4	6	6	7	5	6	8
A ₃	7	9	8	9	8	9	7	8	9	8
A ₄	4	5	6	8	5	4	8	6	8	6
A ₅	2	1	2	1	2	1	2	1	2	1

Вариант 8

K ₁	Эксперты									
Альтернативы	Э ₁	Э ₂	Э ₃	Э ₄	Э ₅	Э ₆	Э ₇	Э ₈	Э ₉	Э ₁₀
A ₁	9	6	8	7	5	4	5	8	9	6
A ₂	4	5	6	8	6	8	4	5	6	4
A ₃	8	9	6	8	4	5	6	8	5	6
A ₄	4	3	2	5	3	6	4	5	3	4
A ₅	4	3	5	3	5	7	6	5	8	6

K ₂	Эксперты									
Альтернативы	Э ₁	Э ₂	Э ₃	Э ₄	Э ₅	Э ₆	Э ₇	Э ₈	Э ₉	Э ₁₀
A ₁	6	7	3	2	3	6	4	5	4	2
A ₂	4	2	6	6	6	5	6	6	5	3
A ₃	9	6	8	7	7	7	6	7	8	6
A ₄	5	4	3	4	4	3	3	2	3	4
A ₅	6	3	5	7	5	7	4	7	4	5

Вариант 9

К ₁	Эксперты									
	Э ₁	Э ₂	Э ₃	Э ₄	Э ₅	Э ₆	Э ₇	Э ₈	Э ₉	Э ₁₀
А ₁	6	8	4	5	8	5	6	8	6	5
А ₂	5	4	6	7	4	5	7	6	4	52
А ₃	9	8	7	8	9	8	7	8	8	8
А ₄	4	5	6	5	4	5	5	5	5	6
А ₅	3	2	3	2	3	2	2	2	3	2

К ₂	Эксперты									
	Э ₁	Э ₂	Э ₃	Э ₄	Э ₅	Э ₆	Э ₇	Э ₈	Э ₉	Э ₁₀
А ₁	5	8	2	4	1	6	4	4	3	2
А ₂	5	4	3	6	4	6	7	5	6	4
А ₃	6	8	4	7	6	5	4	7	5	8
А ₄	5	3	9	6	4	6	3	1	4	3
А ₅	7	6	4	2	8	4	5	6	5	7

7.2.4 Примерный перечень вопросов для подготовки к зачету

Не предусмотрено учебным планом

7.2.5 Примерный перечень заданий для подготовки к экзамену

BS 7799-1:2005 — Британский стандарт BS 7799 первая часть. BS 7799 Part 1 — Code of Practice for Information Security Management (Практические правила управления информационной безопасностью) описывает 127 механизмов контроля, необходимых для построения системы управления информационной безопасностью (СУИБ) организации, определённых на основе лучших примеров мирового опыта (best practices) в данной области. Этот документ служит практическим руководством по созданию СУИБ

BS 7799-2:2005 — Британский стандарт BS 7799 вторая часть стандарта. BS 7799 Part 2 — Information Security management — specification for information security management systems (Спецификация системы управления информационной безопасностью) определяет спецификацию СУИБ. Вторая часть стандарта используется в качестве критериев при проведении официальной процедуры сертификации СУИБ организации.

BS 7799-3:2006 — Британский стандарт BS 7799 третья часть стандарта. Новый стандарт в области управления рисками информационной безопасности Фреймворк "NIST Risk Management Framework". Стандарт NIST SP 800-39 "Managing Information Security Risk". Стандарт NIST SP 800-37 "Risk Management Framework for Information Systems and Organizations". Стандарт NIST SP 800-30 "Guide for Conducting Risk Assessments". Стандарт NIST SP 800-137

"Information Security Continuous Monitoring" . Стандарт ISO/IEC 27005:2018
"Information technology - Security techniques - Information security risk management". Стандарт ISO/IEC 27102:2019 "Information security management - Guidelines for cyber-insurance"

Методология FRAP. Методология OCTAVE. Методология FMEA. Методология CRAMM. Методология FAIR . Методология Microsoft. Концепция COSO ERM

ГОСТ Р ИСО/МЭК 27004-2011 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения

ГОСТ Р ИСО/МЭК 27004-2011 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. Information technology. Security techniques. Information security management. Measurement. Дата введения в действие 01.01.2012.

ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности

ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. Information technology. Security techniques. Information security risk management. Дата введения в действие 01.12.2011.

ГОСТ Р ИСО/МЭК 31010-2011 Менеджмент риска. Методы оценки риска

ГОСТ Р ИСО/МЭК 31010-2011 Менеджмент риска. Методы оценки риска (Risk management. Risk assessment methods). Дата введения в действие: 01.12.2012

ГОСТ Р ИСО 31000-2010 Менеджмент риска. Принципы и руководство
Идентификация активов: описание бизнес-процессов

Идентификация требований безопасности: реестр требований безопасности; требования законодательства и нормативной базы
контрактные обязательства, требования бизнеса

Определение ценности активов: критерии оценки ущерба; таблица ценности активов; особенности интервьюирования бизнес-пользователей

Определение приоритетов аварийного восстановления

Анализ угроз и уязвимостей: профиль и жизненный цикл угрозы; описание угроз безопасности; классификации угроз

уязвимости информационной безопасности; идентификация организационных уязвимостей; идентификация технических уязвимостей;

оценка угроз и уязвимостей

Определение величины риска: калибровка шкалы оценки риска; пример оценки риска. Отчет об оценке рисков

Процесс обработки рисков. Способы обработки риска: принятие риска. уменьшение риска. передача риска. избежание риска

Оценка возврата инвестиций в информационную безопасность

Принятие решения по обработке риска

План обработки рисков
 Декларация о применимости механизмов контроля
 Профили рисков информационной безопасности
 Выбор инструментария для оценки рисков
 Общие недостатки и ограничения коммерческих программных про-
 дуктов
 Обзор методов и инструментальных средств управления рисками

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Экзамен проводится по тест-билетам, каждый из которых содержит 10 вопросов и задачу. Каждый правильный ответ на вопрос в тесте оценивается 1 баллом, задача оценивается в 10 баллов (5 баллов верное решение и 5 баллов за верный ответ). Максимальное количество набранных баллов – 20.

1. Оценка «Неудовлетворительно» ставится в случае, если студент набрал менее 6 баллов.

2. Оценка «Удовлетворительно» ставится в случае, если студент набрал от 6 до 10 баллов

3. Оценка «Хорошо» ставится в случае, если студент набрал от 11 до 15 баллов.

4. Оценка «Отлично» ставится, если студент набрал от 16 до 20 баллов.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Зарубежные стандарты, и фреймворки риск-менеджмента в сфере информационной безопасности	ОПК-3, ПК-4	Тест
2	Методологии риск-менеджмента	ОПК-3, ПК-4	Тест
3	Национальные стандарты Российской Федерации в области защиты информации	ОПК-3, ПК-4	Тест
4	Оценка рисков информационной безопасности	ОПК-3, ПК-4	Тест
5	Обработка рисков информационной безопасности	ОПК-3, ПК-4	Тест
6	Инструментальные средства для управления рисками	ОПК-3, ПК-4	Тест

--	--	--	--

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Фомин, Д. В. Информационная безопасность : учебник / Д. В. Фомин. — Москва: Ай Пи Ар Медиа, 2022. — 222 с. — ISBN 978-5-4497-1548-7. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/118876.html>

Астахов, А. М. Искусство управления информационными рисками / А. М. Астахов. — Саратов : Профобразование, 2017. — 312 с. — ISBN 978-5-4488-0079-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/63803.html>

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

Шаблоны типовых документов по информационной безопасности
<http://securitypolicy.ru/%D1%88%D0%B0%D0%B1%D0%BB%D0%BE%D0%BD%D1%8B>

Государственный реестр сертифицированных средств защиты информации

<https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifika>

tsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00

Банк данных угроз безопасности информации

<https://bdu.fstec.ru/vul>

Международные, национальные (государственные) и отраслевые стандарты в области информационной безопасности (защиты информации), а также информационных технологий и непрерывности бизнеса

<http://www.iso27000.ru/>

Управление рисками ИБ

<https://www.securityvision.ru/blog/upravlenie-riskami-informatsionnoy-bezopasnosti-chast-1-osnovnyye-ponyatiya-i-metodologiya-otsenki-ri/>

Электронная образовательная система ВГТУ

<https://old.education.cchgeu.ru/>

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Аудитория для проведения занятий лекционного и практического типа: аудитория, оснащенная набором демонстрационного оборудования (экран, компьютер, проектор) и оборудованная специализированной учебной мебелью

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Стандартизация и методология управления информационными рисками» читаются лекции.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; пометать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоению учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов

	<p>лекций;</p> <ul style="list-style-type: none"> - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточной аттестации.
<p>Подготовка к промежуточной аттестации</p>	<p>Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом с оценкой три дня эффективнее всего использовать для повторения и систематизации материала.</p>

