Приложение 1

МИНОБРНАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ
Директор института прикладной
математики и компьютерных наук
_____ А.В. Замятин
«_14_» _июня_____ 2023 г.

Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине
(Оценочные средства по дисциплине)

Организационное и правовое обеспечение информационной безопасности

Направление подготовки
09.04.03 Прикладная информатика

Направленность (профиль) подготовки:
Цифровизация государственного и муниципального управления

Томск–2023

ОС составил:
ассистент кафедры компьютерной безопасности _____ В.В. Генрих

Рецензент:
канд. техн. наук, доцент,
заведующий кафедрой компьютерной безопасности С.А. Останин

Оценочные средства одобрены на заседании учебно-методической комиссии института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол №2 от 08.06.2023 г.

Председатель УМК ИПМКН,
д-р техн. наук, профессор _____ С.П. Сущенко

Оценочные средства (ОС) являются элементом системы оценивания сформированности компетенций у обучающихся в целом или на определенном этапе ее формирования.

ОС разрабатываются в соответствии с рабочей программой (РП) дисциплины и включает в себя набор оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине.

1. Компетенции и результаты обучения, формируемые в результате освоения дисциплины

Минимальное требование для выставления «зачета» – достижение сформированности результатов обучения на уровне «отлично»,«хорошо», «удовлетворительно»

Компетенция	**Индикатор компетенции**	**Код и наименование результатов обучения** (планируемые результаты обучения, характеризующие этапы формирования компетенций)	**Критерии оценивания результатов обучения**			
			Отлично (Зачтено)	Хорошо (Зачтено)	Удовлетворительно (Зачтено)	Неудовлетворительно (Не Зачтено)
ПК-1. Способен управлять проектами в области ИТ в условиях неопределенностей, порождаемых запросами на изменения и рисками, с учетом влияния организационного окружения проекта	ИПК-1.3. Управляет рисками в проектах в области ИТ.	ОР-1.3.1 Обучающийся сможет: - использовать нормативные правовые акты в области защиты информации (в т.ч. при реализации/модернизации системы защиты информации объекта информатизации). ОР-1.3.2 Обучающийся сможет: - анализировать основные правовые акты, давать правовую оценку	Управляет рисками в проектах в области ИТ Сформированные системные знания нормативных правовых актов в области защиты информации. Сформированные системные знания правовых основ обеспечения	Управляет рисками в проектах в области ИТ, но допускает неточности Сформированные, но содержащие отдельные пробелы знания нормативных правовых актов в области защиты информации.	Управляет рисками в проектах в области ИТ, но допускает ошибки Общие, но не структурированные знания нормативных правовых актов в области защиты информации.	Не управляет рисками в проектах в области ИТ Фрагментарные знания нормативных правовых актов в области защиты информации. Общие, но не структурированные знания правовых основ обеспечения национальной

		информации, используемой в профессиональной деятельности. ОР-1.3.3 Обучающийся сможет: - подбирать и изучать научно-техническую литературу, изучать и отбирать правовые и нормативные акты в области обеспечения информационной безопасности при проектировании программного обеспечения.	национальной безопасности Российской Федерации; успешно применяемые умения анализировать основные правовые акты и подбирать, и изучать научно-техническую литературу, изучать и отбирать правовые и нормативные акты в области обеспечения информационной безопасности при проектировании программного обеспечения	Сформированные, но содержащие отдельные пробелы знания правовых основ обеспечения национальной безопасности Российской Федерации; успешно применяемые умения анализировать основные правовые акты и подбирать, и изучать научно-техническую литературу, изучать и отбирать правовые и нормативные акты в области обеспечения информационной безопасности при проектировании программного обеспечения	Общие, но не структурированные знания правовых основ обеспечения национальной безопасности Российской Федерации; умения анализировать. умения анализировать основные правовые акты и подбирать, и изучать научно-техническую литературу, изучать и отбирать правовые и нормативные акты в области обеспечения информационной безопасности при проектировании программного обеспечения	безопасности Российской Федерации; умения анализировать, умений анализировать основные правовые акты и подбирать, и изучать научно-техническую литературу, изучать и отбирать правовые и нормативные акты в области обеспечения информационной безопасности при проектировании программного обеспечения

2. Этапы формирования компетенций и виды оценочных средств

№	Этапы формирования компетенций (разделы дисциплины)	Код и наименование результатов обучения	Вид оценочного средства (тесты, задания, кейсы, вопросы и др.)
1.	Введение	ОР-1.3.1, ОР-1.3.2, ОР-1.3.3	конспект самоподготовки, вопросы, опрос на занятиях, коллоквиум, зачет
2.	Лицензирование и оценка соответствия	ОР-1.3.1, ОР-1.3.2, ОР-1.3.3	конспект самоподготовки, вопросы, опрос на занятиях, домашнее задание, коллоквиум, зачет
3.	Технические каналы утечки информации	ОР-1.3.1, ОР-1.3.2, ОР-1.3.3	конспект самоподготовки, вопросы, опрос на занятиях, домашнее задание, зачет
4.	Законодательство в области защиты персональных данных	ОР-1.3.1, ОР-1.3.2, ОР-1.3.3	конспект самоподготовки, вопросы, опрос на занятиях, домашнее задание, зачет

3. Типовые контрольные задания или иные материалы, необходимые для оценки образовательных результатов обучения

3.1. Типовые задания для проведения текущего контроля успеваемости по дисциплине «Организационное и правовое обеспечение информационной безопасности».

Домашние задания:

Задание 1.

Найти и выбрать сертифицированное средство защиты информации (СЗИ), соответствующее заданным параметрам. Описать характеристики выбранного СЗИ, соответствующие определенным нормативными документами ФСБ и ФСТЭК России требованиям.

Задание 2.

Описать возможные технические каналы утечки информации для заданного объекта информатизации и способы их нейтрализации.

Задание 3.

Определить уровень защищенности и актуальные угрозы информационной безопасности для заданной информационной системы персональных данных. Определить перечень мер и средств защиты информации, необходимых для нейтрализации выявленных угроз.

Темы опросов на занятиях:

1. Система обеспечения информационной безопасности Российской Федерации. Регулирование процесса обеспечения информационной безопасности Российской Федерации.
2. Лицензирование в области информационной безопасности. Сертификация средств защиты информации.
3. Аккредитация. Аттестация объектов информатизации.
4. Принципы реализации технических каналов утечки информации.
5. Этапы построения системы защиты информации в организации.
6. Этапы определения уровня защищенности информационных систем персональных данных и актуальных угроз безопасности персональных данных.

Вопросы для коллоквиума:

1. Организационные и правовые меры по защите информации. Государственные органы Российской Федерации в области защиты информации.
2. Основные нормативно-правовые акты в области информационной безопасности.
3. Виды конфиденциальной информации.
4. Лицензирование в области информационной безопасности.
5. Сертификация в области информационной безопасности, нормативно-правовые акты, руководящие документы.
6. Аккредитация в области защиты информации.
7. Аттестация объектов информатизации.

3.2. Типовые задания для проведения промежуточной аттестации по дисциплине «Организационное и правовое обеспечение информационной безопасности».

1. Организационные и правовые меры по защите информации. Государственные органы РФ в области защиты информации.
2. Основные нормативно-правовые акты в области информационной безопасности.
3. Виды конфиденциальной информации.
4. Лицензирование в области информационной безопасности, нормативно-правовые акты.
5. Сертификация в области информационной безопасности, нормативно-правовые акты, руководящие документы.
6. Аккредитация в области защиты информации.
7. Аттестация объектов информатизации.
8. Технические каналы утечки акустической информации.
9. Технические каналы утечки информации, обрабатываемой с использованием основных технических средств и систем.
10. Этапы построения системы защиты информации в организации.
11. Модель угроз информационной безопасности. Основные положения.
12. Модель нарушителя информационной безопасности. Основные положения.

13. Законодательство в области защиты персональных данных. Этапы определения уровня защищенности информационных систем персональных данных.
14. Модель угроз информационной системы персональных данных. Оценка актуальности угроз.

4. Методические материалы, определяющие процедуры оценивания образовательных результатов обучения

Система оценивания предусматривает, что к проводимой в середине семестра оценке текущей успеваемости обучающиеся могут получить только 50% от всего допустимого количества баллов (зачет не учитывается), то есть 40 баллов. За вторую половину семестра студенты могут получить еще 40 баллов. 20 баллов возможно получить на зачете. Итого 80 баллов за семестр (баллы, которые можно получить непосредственно при обучении) и 20 баллов за зачет.

4.1. Методические материалы для оценки текущего контроля успеваемости по дисциплине «Организационное и правовое обеспечение информационной безопасности».

Рейтинговая система для оценки текущей успеваемости обучающихся

Таблица 1 – Балльные оценки для элементов контроля.

Элементы учебной деятельности	Максимальный балл с начала семестра	Оцениваемая компетенция
Конспект самоподготовки	5	ПК-1.
Вопросы	5	ПК-1.
Опрос на занятиях	10	ПК-1.
Домашнее задание	10	ПК-1.
Коллоквиум	10	ПК-1.

Пересчет баллов в оценки текущей успеваемости

Баллы на дату контрольной точки	Оценка
≥ 80% от максимальной суммы баллов	5
От 60% до 79% (включительно) от максимальной суммы баллов	4
От 40% до 59% (включительно) от максимальной суммы баллов	3
<40% от максимальной суммы баллов	2

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине «Организационное и правовое обеспечение информационной безопасности».

Таблица 2 – Балльные оценки для элементов контроля (учтены в т.ч. баллы за текущий контроль успеваемости)

Элементы учебной деятельности	Максимальный балл с начала семестра	Оцениваемая компетенция
Конспект самоподготовки	10	ПК-1.
Вопросы	10	ПК-1.
Опрос на занятиях	20	ПК-1.
Домашнее задание	30	ПК-1.
Коллоквиум	10	ПК-1.
Зачет	20	ПК-1.

Пересчет баллов в оценки промежуточной успеваемости

Баллы на дату контрольной точки	Оценка
≥ 60% от максимальной суммы баллов	зачтено
<60% от максимальной суммы баллов	не зачтено