ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ

Комплексное обеспечение защиты информации объекта информатизации

Код модуля	Модуль
1157412(1)	Комплексное обеспечение защиты информации объекта информатизации

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Астафьева Анна Викторовна	ассистент	Руководитель образовательных программ	Кафедра интеллектуальных информационных технологий
2	Куц Дмитрий Владимирович	без ученой степени, без ученого звания	Старший преподаватель	Учебно-научный центр ”Информационная безопасность”
3	Поршнев Сергей Владимирович	доктор технических наук, профессор	Профессор	Учебно-научный центр ”Информационная безопасность”

Согласовано:

Управление образовательных программ Т.Г. Комарова

Авторы:

- **Астафьева Анна Викторовна, Руководитель образовательных программ, Кафедра интеллектуальных информационных технологий**
- **Куц Дмитрий Владимирович, Старший преподаватель, Учебно-научный центр "Информационная безопасность"**
- **Поршнев Сергей Владимирович, Профессор, Учебно-научный центр "Информационная безопасность"**

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Комплексное обеспечение защиты информации объекта информатизации

1.	**Объем дисциплины в зачетных единицах**	5	
2.	**Виды аудиторных занятий**	Лекции Лабораторные занятия	
3.	**Промежуточная аттестация**	Экзамен	
4.	**Текущая аттестация**	Контрольная работа	1
		Домашняя работа	1

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Комплексное обеспечение защиты информации объекта информатизации

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предъявление должно подтвердить факт освоения предметного содержания данной дисциплины, указанного в табл. 1.3 РПМ-РПД.

Таблица 1

Код и наименование компетенции	**Планируемые результаты обучения (индикаторы)**	**Контрольно-оценочные средства для оценивания достижения результата обучения по дисциплине**
1	**2**	**3**
ПК-12 -Способен администрировать средства защиты информации в компьютерных системах и сетях	З-1 - Идентифицировать архитектуры подсистем защиты информации в операционных системах З-2 - Описать принципы построения компьютерных сетей З-3 - Описать принципы функционирования сетевых протоколов, включающих криптографические алгоритмы	Домашняя работа Контрольная работа Лабораторные занятия Лекции Экзамен

	П-1 - Выполнять работы по обнаружению вредоносного программного обеспечения П-2 - Выполнять работы ликвидации обнаруженного вредоносного программного обеспечения и последствий его функционирования П-3 - Выполнять разработку требований к встроенным средствам защиты информации программного обеспечения У-1 - Настраивать антивирусные средства защиты информации в операционных системах У-2 - Устанавливать обновления программного обеспечения и средств антивирусной защиты У-3 - Формировать шаблоны конфигурации программно-аппаратных средств защиты информации в компьютерных сетях	
ПК-13 -Способен обеспечивать защиту информации при работе с базами данных, при передаче по компьютерным сетям	З-1 - Описать принципы построения систем управления базами данных З-2 - Описать виды политик управления доступом и информационными потоками применительно к прикладному программному обеспечению З-3 - Характеризовать уязвимости используемого программного обеспечения и методы их эксплуатации П-1 - Определять состава применяемых программно-аппаратных средств защиты информации в операционных системах П-2 - Выполнять разработку порядка применения программно-аппаратных средств защиты информации в операционных системах П-3 - Выполнять конфигурирование программно-аппаратных средств защиты	Домашняя работа Контрольная работа Лабораторные занятия Лекции Экзамен

	информации в операционных системах У-1 - Оценивать угрозы безопасности информации в компьютерных сетях У-2 - Настраивать правила фильтрации пакетов в компьютерных сетях У-3 - Обосновывать выбор используемых программно-аппаратных средств защиты информации в компьютерных сетях	

3. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ МОДУЛЯ В БАЛЬНО-РЕЙТИНГОВОЙ СИСТЕМЕ (ТЕХНОЛОГИЧЕСКАЯ КАРТА БРС)

3.1. Процедуры текущей и промежуточной аттестации по дисциплине

1. Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0.6		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
контрольная работа	*7,7*	*100*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.5		
Промежуточная аттестация по лекциям – экзамен **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.5**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – не предусмотрено		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– не предусмотрено		
Промежуточная аттестация по практическим/семинарским занятиям–нет **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– не предусмотрено**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –0.4		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**

домашняя работа	7,14	100
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям -1		
Промежуточная аттестация по лабораторным занятиям –нет **Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям – не предусмотрено**		
4. Онлайн-занятия: коэффициент значимости совокупных результатов онлайн-занятий –не предусмотрено		
Текущая аттестация на онлайн-занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по онлайн-занятиям -не предусмотрено		
Промежуточная аттестация по онлайн-занятиям –нет **Весовой коэффициент значимости результатов промежуточной аттестации по онлайн-занятиям – не предусмотрено**		

3.2. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Текущая аттестация выполнения курсовой работы/проекта	**Сроки − семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент текущей аттестации выполнения курсовой работы/проекта– не предусмотрено		
Весовой коэффициент промежуточной аттестации выполнения курсовой работы/проекта– защиты – не предусмотрено		

4. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

4.1. В рамках БРС применяются утвержденные на кафедре/институте критерии (признаки) оценивания достижений студентов по дисциплине модуля (табл. 4) в рамках контрольно-оценочных мероприятий на соответствие указанным в табл.1 результатам обучения (индикаторам).

Таблица 4

Критерии оценивания учебных достижений обучающихся

Результаты обучения	**Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам**
Знания	Студент демонстрирует знания и понимание в области изучения на уровне указанных индикаторов и необходимые для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Умения	Студент может применять свои знания и понимание в контекстах, представленных в оценочных заданиях, демонстрирует освоение умений на уровне указанных индикаторов и необходимых для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.

Другие результаты	Студент демонстрирует ответственность в освоении результатов обучения на уровне запланированных индикаторов. Студент способен выносить суждения, делать оценки и формулировать выводы в области изучения. Студент может сообщать преподавателю и коллегам своего уровня собственное понимание и умения в области изучения.

4.2 Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении контрольно-оценочных мероприятий по дисциплине модуля) используется универсальная шкала (табл. 5).

Таблица 5

Шкала оценивания достижения результатов обучения (индикаторов) по уровням

Характеристика уровней достижения результатов обучения (индикаторов)				
№ п/п	**Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)**	**Шкала оценивания**		
		Традиционная характеристика уровня		**Качественная характеристика уровня**
1.	Результаты обучения (индикаторы) достигнуты в полном объеме, замечаний нет	Отлично (80-100 баллов)	Зачтено	Высокий (В)
2.	Результаты обучения (индикаторы) в целом достигнуты, имеются замечания, которые не требуют обязательного устранения	Хорошо (60-79 баллов)		Средний (С)
3.	Результаты обучения (индикаторы) достигнуты не в полной мере, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка	Неудовлетворительно (менее 40 баллов)	Не зачтено	Недостаточный (Н)
5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания		Нет результата

5. СОДЕРЖАНИЕ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ПО ДИСЦИПЛИНЕ МОДУЛЯ

5.1. Описание аудиторных контрольно-оценочных мероприятий по дисциплине модуля

5.1.1. Лекции

Самостоятельное изучение теоретического материала по темам/разделам лекций в соответствии с содержанием дисциплины (п. 1.2. РПД)

5.1.2. Лабораторные занятия

Примерный перечень тем

1. Выявление и оценка угроз безопасности информации
2. Определение каналов несанкционированного доступа
3. Оценка эффективности элементов КЗСИ
4. Математическое моделирование элементов КЗСИ
5. Методы оптимизации элементов КЗСИ
6. Оценка экономической эффективности КЗСИ
7. Выявление и оценка угроз безопасности информации

LMS-платформа − не предусмотрена

5.2. Описание внеаудиторных контрольно-оценочных мероприятий и средств текущего контроля по дисциплине модуля

Разноуровневое (дифференцированное) обучение.

Базовый

5.2.1. Контрольная работа

Примерный перечень тем

1. Оценка уровня защищённости ИСПДн
2. Определение категории значимости объекта КИИ
3. Обзор законодательства РФ в сфере защиты персональных данных
4. Обзор законодательства РФ в сфере защиты её критической информационной инфраструктуры
5. Разработка политики информационной безопасности
6. Моделирование угроз безопасности
7. Разработка сценария реализации угрозы ИБ

Примерные задания

1. На основании описания ИСПДн определить уровень её защищённости и сформировать базовый набор мер защиты, в соответствии с регламентирующими документами.
2. На основании описания объекта КИИ определить категорию значимости объекта и сформировать базовый набор мер защиты, в соответствии с регламентирующими документами.
3. Разработать возможный сценарий для реализации угрозы УБИ. 008 БДУ ФСТЭК
4. Разработать возможный сценарий для реализации угрозы УБИ. 009 БДУ ФСТЭК
5. Составить обзор законодательства РФ в сфере защиты персональных данных
6. Составить обзор законодательства РФ в сфере защиты её критической информационной инфраструктуры
7. Заполнить шаблон технического задания на создание системы защиты в соответствии с заданными исходными данными.

LMS-платформа − не предусмотрена

5.2.2. Домашняя работа

Примерный перечень тем

1. Составление комплекта организационно-распорядительной документации для ИСПДн

2. Составление комплекта организационно-распорядительной документации для ЗОКИИ

3. Создание модели угроз для ИСПДн

4. Работа с БДУ ФСТЭК

5. Работа с бюллетенями НКЦКИ

Примерные задания

1. На основании описания организации и подготовленных шаблонов разработать комплект организационно-распорядительной документации для заданной ИСПДн

2. На основании описания организации и подготовленных шаблонов разработать комплект организационно-распорядительной документации для ЗОКИИ

3. На основании описания организации обосновать актуальность / неактуальность угрозы УБИ. 008 БДУ ФСТЭК

4. На основании описания организации, исходных данных и подготовленного шаблона разработать модель угроз для ИСПДн

5. На основании шаблона разработать регламент реагирования на бюллетени НКЦКИ.

LMS-платформа − не предусмотрена

5.3. Описание контрольно-оценочных мероприятий промежуточного контроля по дисциплине модуля

5.3.1. Экзамен

Список примерных вопросов

1. Организационное обеспечение информационной безопасности как составная часть системы комплексного противодействия информационным угрозам.

2. Структура и задачи органов власти и управления, отвечающих за организацию защиты информации в стране.

3. Основные принципы построения организационного обеспечения защиты информации и предъявляемые к ней требования.

4. Основные цели и задачи организационного обеспечения информационной безопасности на предприятии.

5. Объекты и субъекты организационного обеспечения защиты информации коммуникативного процесса.

6. Угрозы информационной безопасности. Виды угроз. Организационные меры противодействия различным видам угроз.

7. Случайные и преднамеренные угрозы. Меры организационного противодействия случайным и преднамеренным угрозам.

8. Случайные и преднамеренные угрозы. Меры организационного противодействия случайным и преднамеренным угрозам.

9. Содержание аналитических документов, необходимых для разработки «Политики информационной безопасности предприятия».

10. Структура и содержание документа «Политика информационной безопасности предприятия».

11. Служба информационной безопасности предприятия. Состав, цели и задачи службы информационной безопасности предприятия.

12. Роль стандартов и требований по информационной безопасности предприятия в формировании «Политики информационной безопасности предприятия». Принципы распределения полномочий.

13. Права и обязанности руководящего состава и сотрудников службы информационной безопасности. Роль служебных комиссий и «кризисных групп» в обеспечении информационной безопасности.

14. Организация доступа и допуска сотрудников к конфиденциальной информации.

15. Порядок допуска предприятий к работам по созданию средств защиты конфиденциальной информации и к работам по оказанию услуг в области защиты конфиденциальной информации.

16. Организация доступа к информационным системам, обрабатывающим конфиденциальную информацию. Матричный и мандатный подходы к проблемам разграничения доступа.

17. Порядок обеспечения сохранности конфиденциальной информации при постоянном или временном прекращении пользователем доступа к конфиденциальному информационному ресурсу.

18. Требования, предъявляемые к претендентам на работу с конфиденциальной информацией и к претендентам на должность службу информационной безопасности.

19. Текущая работа с персоналом, допущенным к конфиденциальной информации. Дисциплинарная ответственность. Меры поощрения и наказания.

20. Организация служебного расследования по фактам утечки конфиденциальной информации.

LMS-платформа − не предусмотрена

5.4 Содержание контрольно-оценочных мероприятий по направлениям воспитательной деятельности

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения	**Контрольно-оценочные мероприятия**
Профессиональное воспитание	учебно-исследовательская, научно-исследовательская целенаправленная работа с информацией для использования в практических целях	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности Технология самостоятельной работы	ПК-13	П-3	Домашняя работа Контрольная работа Лабораторные занятия Экзамен