ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ПО ДИСЦИПЛИНЕ

Безопасность автоматизированных информационно-управляющих систем

Код модуля	**Модуль**
1156870(1)	Защита информации в информационно-управляющих систем

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Гайдамакин Николай Александрович	доктор технических наук, профессор	Профессор	Учебно-научный центр ”Информационная безопасность”
2	Пономарева Ольга Алексеевна	кандидат технических наук, без ученого звания	Доцент	Учебно-научный центр ”Информационная безопасность”
3	Поршнев Сергей Владимирович	д.т.н, профессор	директор Учебно-научного центра "Информационная безопасность"	УНЦ ИБ

Согласовано:

Управление образовательных программ Т.Г. Комарова

Авторы:

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Безопасность автоматизированных информационно-управляющих систем

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

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Безопасность автоматизированных информационно-управляющих систем

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**
ОПК-1 -Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	З-1 - Изложить сущность и понятие информации, информационной безопасности, их роль в современном обществе значение для обеспечения объективных потребностей личности, общества и государства З-2 - Описать психологические аспекты информационной безопасности в современном обществе З-3 - Сделать обзор основных методов обеспечения информационной безопасности П-1 - Иметь практический опыт выбора базовых методов выявления и классификации угроз информационной	Домашняя работа Контрольная работа Лекции Практические/семинарские занятия Экзамен

	безопасности современного общества, основными подходами к противодействию угрозам информационной безопасности У-1 - Работать с различными источниками информации У-2 - Осуществлять сбор и анализ полученной информации У-3 - Систематизировать и классифицировать полученную информацию	
ПК-5 -Способен разработать и смоделировать программно-технические средства защиты информации от несанкционированного доступа (Информационная безопасность телекоммуникационных систем)	З-1 - Различать стандарты ЕСКД, ЕСТД и ЕСПД З-10 - Характеризовать средства проектирования электронных схем З-2 - Характеризовать современные информационные технологии (операционные системы, базы данных, вычислительные сети) З-3 - Характеризовать способы реализации несанкционированного доступа к информации и специальных программных воздействий на информацию и ее носители в автоматизированных системах З-4 - Различать основные классы и виды уязвимостей программного обеспечения З-5 - Объяснять методы и технологии защиты информации от несанкционированного доступа и специальных программных воздействий на нее З-6 - Характеризовать (программно-технические) средства защиты автоматизированных систем от несанкционированного доступа к информации и специальных программных воздействий на нее З-7 - Характеризовать методы контроля защищенности информации от несанкционированного доступа	Домашняя работа Контрольная работа Лекции Практические/семинарские занятия Экзамен

	и специальных программных воздействий З-8 - Характеризовать средства контроля защищенности информации от несанкционированного доступа З-9 - Характеризовать методики контроля защищенности информации от несанкционированного доступа П-1 - Иметь опыт практической разработки технического (эскизного) проекта программно-технических средств защиты информации от несанкционированного доступа и специальных воздействий на нее П-2 - Иметь опыт практического испытания программно-технических средств защиты информации от несанкционированного доступа и специальных воздействий на нее П-3 - Иметь опыт практической разработки рабочей и эксплуатационной документации на техническое средство защиты У-1 - Составлять техническое задание на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее У-2 - Составлять проектно-сметную документацию на создание программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее У-3 - Составлять программы и методики испытаний программно-технического средства защиты информации от несанкционированного доступа и специальных воздействий на нее	

ОПК-6 -Способен при решении профессиональных задач проверять выполнение требований защиты информации ограниченного доступа в информационно-аналитических системах в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	З-1 - Различать правовые и организационные меры защиты информации, в том числе информации ограниченного доступа З-2 - Изложить содержание нормативных правовых актов, нормативных и методических документов уполномоченных федеральных органов исполнительной власти (в том числе Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю) по защите информации П-1 - Осуществлять обоснованный выбор нормативной базы в области защиты информации ограниченного доступа У-1 - Систематизировать и классифицировать организационно-распорядительные документы, регламентирующие защиту информации ограниченного доступа в автоматизированных системах	Домашняя работа Контрольная работа Лекции Практические/семинарские занятия Экзамен

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 – 0.7**		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
контрольная работа	10,5	*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 – 0.3		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
домашняя работа	10,14	100
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 1		
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 –не предусмотрено		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям -не предусмотрено		
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. Практические/семинарские занятия

Примерный перечень тем

1. Свойства информации. Виды, источники и носители защищаемой информации
2. Средства управления доступом. Классификация и характеристика охранных, охранно- пожарных и пожарных извещателей
3. Средства видеоконтроля и видеоохраны. Средства нейтрализации угроз.
4. Средства управления и передачи извещений.
5. Автоматизированные интегральные системы охраны.
6. Методы технического контроля. Особенности инструментального контроля эффективности инженерно-технической защиты информации
7. Средства подавления сигналов акустоэлектрических преобразователей, фильтрации и заземления

Примерные задания

1. Подготовить обзор литературы по теме практического занятия
2. Структурировать изученный материал по теме практических занятий
3. Сформулировать вопросы по теме практического занятия

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. Закладные устройства, средства ВЧ- навязывания и лазерного подслушивания

2. Модели злоумышленника

3. Разработка математической модели обнаружения атаки

Примерные задания

1.Поясните отличие автоматизированной системы от информационной системы

а) -автоматизированная система что-то автоматизирует, а информационная система осуществляет

б) -информационное обеспечение чего-либо

в)-информация в АС может быть представлена в любой организационно-технологической форме (в виде сигналов, файлов, сообщений, документов и т.д.), информация в ИС представлена в виде базы данных

В определении АС отметьте недостающее - "АС— система, состоящая из _____ и комплекса средств автоматизации_____, реализующая информационную технологию _____ "

а) …базы данных … различных процессов , ….решения задач персонала

б) …персонала …его деятельности ,… выполнения функций

в) …программного обеспечения … различных процессов , …решения управленческих задач

3. Приведите основные разновидности автоматизированных систем по ГОСТ 34.003-90

а) автоматизированные системы процессов, автоматизированные системы подготовки документов,

автоматизированные системы поддержки принятия решений

б) автоматизированные системы управления (АСУТП, АСУП − ERP-системы, АСУПр); системы

автоматизированного проектирования (САПР, CASE-системы); автоматизированные системы

обработки информации (АСОИ, АСОД) и др

в) АС в защищенном исполнении (АСЗИ), автоматизированные банки данных

4. Чем база данных (БД) отличается от совокупности данных, например набора файлов?

а) база данных в отличии от совокупности данных характеризуется структурой в рамках определенной

модели данных, выражаемой некоторым (формальным) языком описания данных

б) то по сути дела одно и то же

в) различной терминологией, употреблямой в сферах баз данных и операционых систем (их файловых

систем)

5. Поясните различия между базой данных и банком данных

а) это практически тождественные понятия, различия между ними сугубо исторические

б) банком данных называют совокупность базы (баз) данных, СУБД и прикладной части в виде

автоматизированных процедур обработки данных, развернутых на СВТ (на технических средствах ввода,

хранения, обработки и выдачи информации)

в) банк данных представляет собой интегрированную БД или совокупность БД на главной вычислительной установке

6. Поясните понятие целостности информации (данных)

а) состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется

только преднамеренно субъектами, имеющими на него право

б) состояние информации (данных), при котором ее содержание (значения данных) и структура не

содержат :

- или нарушений установленных правил или ограничений [по типам, значениям, соотношениям и т.п.];

- и (или) ошибок [логических, семантических];

- и (или) искажений, отклонений от требуемого эталона

в) наличием всех необходимых для функционирования АС данных

7. Перечислите основные принципы обеспечения компьютерной безопасности

а) принципы открытости, совместимости, эффективности, разумной достаточности, сочетания

унификации и оригинальности

б) принципы закрытости, доступности, целостности, разумной достаточности

в) принципы комплексности, системности, разумной достаточности, целенаправленности, сочетания

унификации и оригинальности, непрерывности, управляемости и контроля эффективности

8. Дополните недостающим определение доступности данных - такое состояние информации, при

котором отсутствуют _____ обладателем или уполномоченными лицами

а) преграды доступа к информации и ее обработке

б) препятствия доступа к информации и закономерному ее использованию

в) отказы в доступе к данным и препятствия в обработке данных

LMS-платформа − не предусмотрена

LMS-платформа − не предусмотрена

5.2.2. Домашняя работа

Примерный перечень тем

1. Средства управления доступом. Классификация и характеристика охранных, охранно- пожарных и пожарных извещателей

2. Средства видеоконтроля и видеоохраны. Средства нейтрализации угроз.

3. Средства управления и передачи извещений

4. Автоматизированные интегральные системы охраны.

5. Методы технического контроля. Особенности инструментального контроля эффективности инженерно-технической защиты информации

6. Средства подавления сигналов акустоэлектрических преобразователей, фильтрации и заземления

Примерные задания

1. Отчет формируется на каждую практическую работу

2. К каждой практической работе должно быть описание решаемой задачи, теоретические аспекты решения задачи и описано решение задачи.

3. Каждый этап работы фиксируется снимками экрана и описанием содержимого на экране.

4. По результатам каждой работы формируется отчет

LMS-платформа − не предусмотрена

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

5.3.1. Экзамен

Список примерных вопросов

1. Понятие, виды и структура автоматизированных систем (по РД 50-680-88)

2. Безопасность АС, ее составляющие. Основные способы и механизмы обеспечения безопасности информации в АС

3. Классификация, идентификация (инвентаризация, каталогизация) и оценивание (категорирование) объектов защиты в АС

4. Классификация (каталогизация), идентификация, спецификация и оценивание угроз безопасности в АС

5. Человеческий фактор в угрозах безопасности. Модель нарушителя безопасности информации в АС (РД Гостехкомиссии)

6. Декомпозиция назначения, целей и задач функционирования АС. Функциональная структура АС и функциональные требования к защищенным СВТ, АС, продуктам и системам ИТ

7. Система и структура функциональных требований по защите от НСД к информации в СВТ (по РД Гостехкомиссии), классы защищенности СВТ

8. Система и структура функциональных требований по защите от НСД в АС (по РД Гостехкомиссии), группы и классы защищенности АС

9. Общая структура требований безопасности к изделиям и системам ИТ, классы функциональных требований безопасности (по ГОСТ Р ИСО/МЭК 15408-2002. Ч.2)

10. Услуги (сервисы) безопасности при взаимодействии открытых систем и механизмы безопасности, их реализующие (по ГОСТ Р ИСО 7498-1-99), взаимоотношение между услугами защиты и уровнями взаимодействия по 7-уровневой эталонной модели ВОС

11. Жизненный цикл, стадии создания и содержание работ по созданию АС, особенности создания АС в защищенном исполнении (по ГОСТ 34.601-90, ГОСТ Р 51583)

12. Техническое задание на создание АС, требования по структуре, содержанию, порядку разработки, оформления, согласования и утверждения (по ГОСТ 34.602-89)

13. Особенности Технического задания на создание АС в защищенном исполнении. Составляющие общих требований к АСЗИ и структуру функциональных требований (по ГОСТ Р 51624)

14. Жизненный цикл изделий (продуктов и систем) ИТ, общая схема и последовательность создания изделий ИТ

15. Классификация изделий ИТ и функциональные пакеты требований безопасности. Классы защищенности изделий ИТ и пакеты требований доверия безопасности (по ГОСТ Р ИСО/МЭК 15408-2002 и РД Гостехкомиссии)

16. Структура, порядок разработки, регистрации и опубликования профилей защиты для изделий ИТ (по ГОСТ Р ИСО/МЭК 15408-2002 и РД Гостехкомиссии)

17. Структура, назначение и порядок разработки задания по безопасности при создании изделий ИТ, соотношение между профилем защиты и заданием по безопасности.

18. Техническое задание на создание системы ИТ (по ГОСТ Р ИСО/МЭК 15408-2002 и РД Гостехкомиссии)

19. Содержание процесса разработки и ввода в действие изделий (систем) ИТ. Уровни представления проектных решений

20. Проектирование АС как особый вид деятельности, объекты проектирования при создании АС (по РД 50-680-88)

21. Методология (методы и средства) проектирования АС

22. Каноническое (индивидуальное) проектирование АС. Технологическая схема этапов технического и рабочего проектирования

23. Типовое проектирование АС и его методы. Технологическая схема проектирования Управление процессом проектирования АС, его компоненты и специфика

24. Организационная структура, схемы организации работ при проектировании АС и организационные формы проектного коллектива

25. Содержание и специфика управленческого цикла при проектировании АС

26. Методы планирования и управления проектами. Диаграммы Гантта, сетевые графики проектов

27. Автоматизированные системы управления проектами Общие положения по эксплуатации изделий, комплексов, средств деятельности

28. Составляющие организационных и технических мероприятий по эксплуатации Особенности эксплуатации КС (АС) и защищенных КС (АС в защищенном исполнении). Администрирование КС (АС)

29. Органы управления и планирования эксплуатации защищенных АС Эксплуатационная документация на АС (изделия ИТ). Руководства пользователя и администратора

30. Конструкторские эксплуатационные документы на ТСО и ПО, эксплуатационные документы предприятия

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-	Технология самостоятельной работы	ОПК-6	З-1	Домашняя работа Контрольная работа

	исследовательская				Практические/семинарские занятия Экзамен