Федеральное агентство по рыболовству
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
(ФГБОУ ВО «КГТУ»)

УТВЕРЖДАЮ
Начальник УРОПСП

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
ФГБОУ ВО «КГТУ»
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат:
0174a99400e2af6fb74dca3b394e65efc4
Владелец: Мельникова Виктория Александровна
Действителен: с 12.04.2023 по 12.04.2024

Фонд оценочных средств
(приложение к рабочей программе модуля)

«ИНТЕГРИРОВАННЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ»

основной профессиональной образовательной программы специалитета
по специальности

10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация

«БЕЗОПАСНОСТЬ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»

ИНСТИТУТ	Институт цифровых технологий
РАЗРАБОТЧИК	Кафедра информационной безопасности

1 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Таблица 1 – Планируемые результаты обучения по дисциплине, соотнесенные с установленными индикаторами достижения компетенций

Код и наименование компетенции	Индикаторы достижения компетенции	Дисциплина	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
ОПК-9: Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ОПК-9.2: Знает виды, функциональные возможности, принципы организации интегрированных систем безопасности ОПК-9.3: Умеет решать вопросы анализа угроз физической безопасности объекта и моделей потенциальных нарушителей, физические принципы обнаружения человека. Знает принципы построения распределенных систем охранно-пожарной сигнализации, систем управления контроля и разграничения доступом, систем телевизионного наблюдения, автономных и централизованных интегрированных комплексов охраны. Знает вопросы тактики применения технических средств охраны на объектах различного назначения	Интегрированные системы безопасности	*Знает*: методологию проектирования интегрированных систем безопасности с учетом их функционального назначения и объекта установки (применения); требования, предъявляемые к средствам отображения информации, органам управления систем безопасности; особенности проектирования ИСБ различного функционального назначения; принципы проектирования интегрированных систем безопасности. *Умеет:*. проектировать ИСБ с учётом вида объекта решаемых задач и условий работы системы; определять номенклатуру, характеристики и проводить выбор типов технических средств, используемых в составе ИСБ (датчиков, исполнительных устройств и т.д.); осуществлять выбор и проектирование каналов передачи информации для обеспечения взаимосвязи и взаимодействия между частями ИСБ и оператором; выполнять размещение (компоновку) частей ЭСБ на объекте с учётом особенностей самого объекта, характера решаемых системой задач, возможностей операторов; выполнять оценку эффективности функционирования ИСБ конкретного функционального назначения.

Код и наименование компетенции	Индикаторы достижения компетенции	Дисциплина	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
			Владеет: навыками разработки и создания ИСБ; навыками оценки эффективности созданных ИСБ и анализа угроз в ИСБ.

2 ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПОЭТАПНОГО ФОРМИРОВАНИЯ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ (ТЕКУЩИЙ КОНТРОЛЬ) И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

2.1 Для оценки результатов освоения дисциплины используются:

- оценочные средства текущего контроля успеваемости;

- оценочные средства для аттестации по дисциплине.

2.2 К оценочным средствам для текущего контроля успеваемости относятся:

- задания и контрольные вопросы по лабораторным работам;

- тестовые задания.

2.3 К оценочным средствам для промежуточной аттестации по дисциплине проводимой в форме экзамена, относятся:

- вопросы на экзамен.

3 ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

3.1 Задания и контрольные вопросы по лабораторным работам. Дисциплина «Интегрированные системы безопасности» изучается 1 семестр и состоит из 4 разделов.

3.1.1 Задания по разделу: «Общие принципы организации защиты объектов информатизации»:

- Классификация предметов защиты и объектов охраны;

- Классификация нарушителей и потенциальных угроз безопасности;

- Основы формирования комплекса технических средств обеспечения безопасности;

- Структура комплексной системы безопасности. Общие принципы построения систем безопасности;

- Зоны обеспечения безопасности. Условия функционирования систем безопасности.

3.1.2 Задания по разделу: «Интегрированные системы безопасности: общие сведения»:

- Классификация ИСБ;

- Принципы организации ИСБ;

- Структурные схемы ИСБ. Существующие ИСБ.

3.1.3 Задания по разделу: «Компоненты интегрированных систем безопасности»:

- Системы охранной, тревожной и пожарной сигнализации;

- Системы контроля и управления доступом;

- Системы охранного телевидения.

3.1.4 Контрольные вопросы по разделу «Проектирование систем безопасности»:

- Жизненный цикл систем безопасности

- Процедура проектирования систем безопасности

- Выбор оборудования для системы безопасности

- Выбор вариантов охраны объекта

- Методы оценки эффективности систем безопасности.

3.1.5 Критерии оценки лабораторной работы:

- оценка «зачтено» выставляется обучающемуся, если он демонстрирует способность к полной самостоятельности (допускаются консультации с преподавателем по сопутствующим вопросам) в выборе способа решения неизвестных или нестандартных заданий в рамках учебной дисциплины с использованием знаний, умений и навыков, полученных как в ходе освоения данной учебной дисциплины, так и смежных дисциплин;

- оценка «незачтено» выставляется, если выявляется неспособность обучаемого самостоятельно продемонстрировать наличие знаний при решении заданий, которые были представлены преподавателем вместе с образцом их решения, отсутствие самостоятельности в применении умения к использованию методов освоения учебной дисциплины и неспособность самостоятельно проявить навык повторения решения поставленной задачи по стандартному образцу, что свидетельствует об отсутствии сформированной компетенции.

3.2. Тестовые задания

3.2.1. Тестовые задания представлены ниже (ключи к ним – в Приложении № 1):

Вариант 1

Вопрос 1: Размер объектов, на которых традиционно применяются ИСБ: 1) большие; 2) средние; 3) мелкие.
Вопрос 2: Матрица угроз для объектов с ИСБ имеет структуру: 1) простую; 2) сложную; 3) смешанную;
Вопрос 3: Главное преимущество ИСБ это:

1) информационное объединение систем и, как следствие, предоставление единого интерфейса взаимодействия с информационными системами предприятия; 2) возможность собирать информацию от датчиков; 3) возможность производить видеонаблюдение помещений предприятия; 4) возможность организовать вызов экстренных служб.
Вопрос 4: Способность объединять разнородные технические системы и средства в ИСБ: 1) не существует; 2) существует частично; 3) существует полностью.
Вопрос 5: «Информация» это: 1) совокупность содержащихся в базах данных сведений; 2) совокупность содержащихся в базах данных сведений, зафиксированных на машинных носителях; 3) сведения (сообщения, данные) воспроизводимые различными системами; 4) сведения (сообщения, данные) независимо от формы их представления.
Вопрос 6: «Несанкционированный доступ к информации» это доступ: 1) реализующий возможности совокупности физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация; 2) к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств; 3) с использованием совокупности средств технической разведки и прочих средств, которыми добывается защищаемая информация; 4) к информации, реализуемый путём уничтожения технических средств информационной системы.
Вопрос 7: Модуль безопасности, не относящийся к базовым модулям ИСБ: 1) видеонаблюдение; 2) сопровождение удаленной работы сотрудников; 3) пожарно-охранная сигнализация; 4) СКУД; 5) система контроля телекоммуникациями;
Вопрос 8: Недостатком традиционных систем безопасности являются: 1) масштабируемость; 2) надежность 3) сравнительно небольшая стоимость 4) информационная перегрузка оператора 5) сложность в исполнении
Вопрос 9: Наиболее эффективная система пожарной сигнализации (раннее обнаружение очага): 1) классические пожарные извещатели; 2) датчики пожаротушения; 3) видеоаналитические решения;
Вопрос 10: Элементы простой системы видеонаблюдения**:** 1) Три ТВ камеры и видеомонитор 2) ТВ камера и несколько видеомониторов 3) ТВ камера, видеомонитор и видео коммутатор 4) ТВ камера и видеомонитор
Вопрос 11: Угол обзора видеокамеры зависит от: 1) размера матрицы; 2) фокусного расстояния объектива; 3) обоих параметров;

Вопрос 12: Важный элемент классификации данных, продуманный начальством: 1) типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным; 2) необходимый уровень доступности, целостности и конфиденциальности; 3) оценить уровень риска и отменить контрмеры; 4) управление доступом, которое должно защищать данные.
Вопрос 13: Наименее важным фактором для уверенности в том, что безопасность в компании обеспечена успешно, является: 1) поддержка высшего руководства; 2) эффективные защитные меры и методы их внедрения; 3) Актуальные и адекватные политики и процедуры безопасности; 4) проведение тренингов по безопасности для всех сотрудников.
Вопрос 14: К рекомендуемым методам и способам защиты информации в информационных системах относятся методы и способы: 1) защиты информации от несанкционированного доступа; 2) сокрытия информации от внутренних нарушителей; 3) устранения конкурентов; 4) защиты информации от утечки по техническим каналам.
Вопрос 15: Защита информации это: 1) процесс сбора, накопления, обработки, хранения, распределения и поиска информации; 2) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа; 3) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств; 4) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям; 5) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

Вариант 2

Вопрос 1: Наиболее эффективная система пожарной сигнализации (раннее обнаружение очага): 1) классические пожарные извещатели; 2) датчики пожаротушения; 3) видеоаналитические решения;
Вопрос 2: «Несанкционированный доступ к информации» это доступ: 1) реализующий возможности совокупности физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация; 2) к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств; 3) с использованием совокупности средств технической разведки и прочих средств, которыми добывается защищаемая информация; 4) к информации, реализуемый путём уничтожения технических средств информационной системы.
Вопрос 3: Традиционные размеры объектов для применения стандартных ИСБ: 1) большие; 2) средние; 3) мелкие.
Вопрос 4: Не базовым модулем безопасности ИСБ является: 1) видеонаблюдение; 2) сопровождение удаленной работы сотрудников;

3) пожарно-охранная сигнализация; 4) СКУД; 5) система контроля телекоммуникациями.
Вопрос 5: Матрица угроз для объектов ИСБ имеет структуру: 1) простую; 2) сложную; 3) смешанную;
Вопрос 6: Защита информации это: 1) процесс сбора, накопления, обработки, хранения, распределения и поиска информации 2) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа 3) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств 4) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям 5) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.
Вопрос 7: Активными способами защиты информации являются: 1) Ослабление проникновения информационных сигналов в цепи электропитания аппаратных средств ИСПДн, выходящие за пределы контролируемой зоны; 2) Создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях технических средств; 3) Ослабление ПЭМИ; 4) Правильная разработка организационно-распорядительной документации для обеспечения информационной безопасности.
Вопрос 8: К рекомендуемым методам и способам защиты информации в информационных системах относятся методы и способы: 1) защиты информации от несанкционированного доступа; 2) сокрытия информации от внутренних нарушителей; 3) устранения конкурентов; 4) защиты информации от утечки по техническим каналам.
Вопрос 9: Для контроля защищенности информации применяются средства: 1) Рекомендованные ФСТЭК России; 2) Рекомендованные ФСБ России; 3) Рекомендованные Роскомнадзором; 4) прошедшие в установленном законом порядке процедуру оценки соответствия.
Вопрос 10: Наименее важным фактором для уверенности в том, что безопасность в компании обеспечена успешно, является: 1) поддержка высшего руководства; 2) эффективные защитные меры и методы их внедрения; 3) актуальные и адекватные политики и процедуры безопасности; 4) проведение тренингов по безопасности для всех сотрудников.
Вопрос 11: Важный элемент классификации данных, продуманный начальством: 1) типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным; 2) необходимый уровень доступности, целостности и конфиденциальности; 3) оценить уровень риска и отменить контрмеры; 4) управление доступом, которое должно защищать данные.
Вопрос 12: «Информация» это: 1) совокупность содержащихся в базах данных сведений;

2) совокупность содержащихся в базах данных сведений, зафиксированных на машинных носителях; 3) сведения (сообщения, данные) воспроизводимые различными системами; 4) сведения (сообщения, данные) независимо от формы их представления.
Вопрос 13: Главное преимущество ИСБ это: 1) информационное объединение систем и, как следствие, предоставление единого интерфейса взаимодействия с информационными системами предприятия; 2) возможность собирать информацию от датчиков; 3) возможность производить видеонаблюдение помещений предприятия; 4) возможность организовать вызов экстренных служб.
Вопрос 14: Способность объединять разнородные технические системы и средства в ИСБ: 1) не существует; 2) существует частично; 3) существует полностью.
Вопрос 15: Самым эффективным способом аутентификации является: 1) биометрические данные; 2) пароль; 3) смарт-карты; 4) двухфакторная аутентификация.

Вариант 3

Вопрос 1: Активными способами защиты информации являются: 1) Ослабление проникновения информационных сигналов в цепи электропитания аппаратных средств ИСПДн, выходящие за пределы контролируемой зоны; 2) Создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях технических средств; 3) Ослабление ПЭМИ; 4) Правильная разработка организационно-распорядительной документации для обеспечения информационной безопасности.
Вопрос 2: К рекомендуемым методам и способам защиты информации в информационных системах относятся методы и способы: 1) защиты информации от несанкционированного доступа; 2) сокрытия информации от внутренних нарушителей; 3) устранения конкурентов; 4) защиты информации от утечки по техническим каналам.
Вопрос 3: Наименее важным фактором для уверенности в том, что безопасность в компании обеспечена успешно: 1) поддержка высшего руководства; 2) эффективные защитные меры и методы их внедрения; 3) актуальные и адекватные политики и процедуры безопасности; 4) проведение тренингов по безопасности для всех сотрудников.
Вопрос 4: Формирование требований к защите информации, содержащейся в информационной системе, согласно 17 приказа ФСТЭК, осуществляется: 1) обладателем информации (заказчиком); 2) владельцем информации; 3) организацией, имеющей лицензию на техническую защиту информации; 4) организацией, имеющей лицензию на криптографическую защиту информации;
Вопрос 5: Способность объединять разнородные технические системы и средства в ИСБ: 1) не существует; 2) существует частично;

3) существует полностью.
Вопрос 5: Матрица угроз для объектов ИСБ имеет структуру: 1) простую; 2) сложную; 3) смешанную.
Вопрос 7: Не базовым модулем безопасности ИСБ является: 1) видеонаблюдение; 2) сопровождение удаленной работы сотрудников; 3) пожарно-охранная сигнализация; 4) СКУД; 5) система контроля телекоммуникациями.
Вопрос 8: Для контроля защищенности информации применяются средства: 1) рекомендованные ФСТЭК России; 2) рекомендованные ФСБ России; 3) рекомендованные Роскомнадзором; 4) прошедшие в установленном законом порядке процедуру оценки соответствия.
Вопрос 9: Наименее важным фактором для уверенности в том, что безопасность в компании обеспечена успешно: 1) поддержка высшего руководства; 2) эффективные защитные меры и методы их внедрения; 3) актуальные и адекватные политики и процедуры безопасности; 4) проведение тренингов по безопасности для всех сотрудников.
Вопрос 10: Главное преимущество ИСБ это: 1) информационное объединение систем и, как следствие, предоставление единого интерфейса взаимодействия с информационными системами предприятия; 2) возможность собирать информацию от датчиков; 3) возможность производить видеонаблюдение помещений предприятия; 4) возможность организовать вызов экстренных служб.
Вопрос 11: Контроль состояния защиты информации отраслевыми и федеральными органами заключается в оценке: 1) соблюдения требований нормативно-методических документов по защите информации; 2) соблюдения требований отраслевых стандартов; 3) работоспособности применяемых средств защиты информации в соответствии с их эксплуатационной документацией; 4) соблюдения требований Трудового кодекса РФ; 5) знаний и выполнения персоналом своих функциональных обязанностей в части защиты информации.
Вопрос 12: Активными способами защиты информации являются: 1) ослабление проникновения информационных сигналов в цепи электропитания аппаратных средств ИСПДн, выходящие за пределы контролируемой зоны; 2) создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях технических средств; 3) ослабление ПЭМИ; 4) правильная разработка организационно-распорядительной документации для обеспечения информационной безопасности.
Вопрос 13: «Контролируемая зона» это:

1) пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств; 2) часть здания, в котором исключено неконтролируемое пребывание посторонних лиц, транспортных, технических и иных материальных средств; 3) пространство (территория, здание, часть здания, помещение), в котором действует особый режим наблюдения за всеми сотрудниками организации; 4) помещение, в котором постоянно, независимо от окружающих факторов ведётся систематический контроль и надзор за действиями пользователей.
Вопрос 11: Угол обзора камеры зависит от: 1) размера матрицы; 2) фокусного расстояния объектива; 3) обоих параметров;
Вопрос 15: «Специальные исследования (специсследования)» это: 1) выявление с помощью контрольно-измерительной аппаратуры возможных каналов утечки информации ограниченного доступа, обрабатываемой техническими средствами; 2) определение соответствия условий эксплуатации объектов информатизации требованиям аттестатов соответствия, и других руководящих документов по спецзащите без применения контрольно-измерительной аппаратуры; 3) проверки технических средств иностранного и совместного производства на наличие возможно внедренных электронных устройств перехвата информации.

3.2.4 Критерии оценивания тестовых заданий:

«зачтено» - 75-100% верных ответов;

«незачтено» - 0-74% верных ответов;

4 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

4.1 Аттестация по дисциплине проводится в форме экзамена.

4.1.1 Вопросы к экзамену:

1. Классификация предметов защиты и объектов охраны.
2. Классификация потенциальных угроз безопасности.
3. Классификация потенциальных нарушителей безопасности.
4. Основы формирования комплекса технических средств обеспечения безопасности.
5. Основные термины и определения в области интегрированных систем безопасности
6. Структура комплексной системы безопасности.
7. Общие принципы построения систем безопасности.
8. Зоны обеспечения безопасности.
9. Условия функционирования систем безопасности.
10. Классификация ИСБ.

11. Принципы организации ИСБ.
12. Структурные схемы ИСБ.
13. Системы охранной, тревожной и пожарной сигнализации.
14. Системы контроля и управления доступом.
15. Системы охранного телевидения.
16. Жизненный цикл систем безопасности.
17. Процедура проектирования систем безопасности.
18. Выбор оборудования для системы безопасности.
19. Выбор вариантов охраны объекта.
20. Методы оценки эффективности систем безопасности
21. Взрывобезопасность уникальных объектов.
22. Защита объекта от террористических угроз.
23. Риск обрушения объекта. Ликвидация последствий обрушения.
24. Внешние и внутренние угрозы безопасности ИСБ
25. Внешние и внутренние нарушителя ИСБ
26. Сравнительный анализ существующих ИСБ на рынке

4.2 Критерии оценивания промежуточной аттестации:

Оценка **“отлично”** на экзамене выставляется студенту, который:

- дал полный ответ на два вопроса.
- при ответе на дополнительные вопросы показал знание всех разделов курса.

Оценка **“хорошо”** на зачете выставляется студенту, который:

- дал ответ на два вопроса, за исключением наиболее трудных. Допускает незначительные неточности в доказательствах.
- при ответе на дополнительные вопросы показал знание всех разделов курса.

Оценка **“удовлетворительно”** на зачете выставляется студенту, который:

- дал ответ на два вопроса. Допускает неточности и пробелы в формулировках, не нарушающие общей логики рассуждений.
- при ответе на дополнительные вопросы показал знание основных понятий и наиболее важных законов программы курса.

Оценка **“неудовлетворительно”** выставляется студенту, который:

- при ответе на вопросы допускает грубые ошибки.
- отвечая на дополнительные вопросы, демонстрирует существенные пробелы в знаниях.

СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

Фонд оценочных средств для аттестации по дисциплине «Интегрированные системы безопасности» представляет собой компонент основной профессиональной образовательной программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация «Безопасность открытых информационных систем»).

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры информационной безопасности 20.04.2022 г. (протокол № 7).

Заведующая кафедрой  Н.Я.Великите