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)

«ПРОЕКТИРОВАНИЕ ОТКРЫТЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ»

основной профессиональной образовательной программы специалитета по специальности

10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация

«БЕЗОПАСНОСТЬ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»

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-5.1: Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем; ОПК-5.2: Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем; ОПК-5.3: Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах.	ОПК-5.1$_{ИД1}$: Знает основные угрозы безопасности информации и модели нарушителя в открытых информационных системах на основе руководящих и методические документов уполномоченных федеральных органов исполнительной власти по защите информации; ОПК-5.1$_{ИД2}$: Знает принципы организации и структуру систем защиты информации программного обеспечения автоматизированных систем; ОПК-5.2$_{ИД4}$: Умеет выбирать меры защиты информации, подлежащие реализации в системе защиты информации открытых информационных систем, проектировать подсистемы	Проектирование открытых систем в защищённом исполнении	*Знать:* общие принципы построения открытых систем в защищенном исполнении, принципы проектирования архитектуры, структуры и основных объектов защищенных систем; основные этапы процесса проектирования и методы, используемые при построении проектируемой сети; способы нарушения информационной безопасности при работе автоматизированных систем обработки информации; особенности политики безопасности и способы ее внедрения на предприятии; методики оценки качества предлагаемых решений в области информационной безопасности. *Уметь:* формировать требования к проектируемой сети с учетом анализа угроз и несанкционированных воздействий; составлять функциональные схемы проектируемых информационных систем; выявлять возможные способы нарушения информационной безопасности при работе автоматизированных систем обработки информации и описывать их с учетом методических рекомендаций регуляторов с области защиты информации; определять

Код и наименование компетенции	Индикаторы достижения компетенции	Дисциплина	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
	безопасности информации с учетом действующих нормативных и методических документов, разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем; ОПК -5.З$_{ИД2}$: Знает угрозы безопасности, информационные воздействия, критерии оценки защищенности и методы защиты информации в открытых информационных системах, умеет исследовать эффективность проектных решений программно-аппаратных средств обеспечения защиты информации в автоматизированной системе с целью обеспечения требуемого уровня защищенности.		задачи обеспечения информационной безопасности с учетом требований нормативно-правовых актов; в рамках задач обеспечения информационной безопасности решать вопросы использования средств защиты информации с учетом требований нормативно-правовых актов регуляторов; определять особенности политики безопасности и способы ее внедрения на предприятии с учетом требований нормативно-правовых актов; давать оценку качества предлагаемых решений в области информационной безопасности; применять системный подход к обеспечению информационной безопасности в различных сферах деятельности, включая комплекс организационных мер. *Владеть:* методами построения открытых систем в защищенном исполнении; навыками составления проекта и пониманием содержания основных этапов процесса проектирования; методиками определения задач обеспечения информационной безопасности; политиками безопасности и способами ее внедрения на предприятии; методиками оценки качества предлагаемых решений в области информационной безопасности

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 промежуточной 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 курсового проекта, дифференцированного зачета и экзамена, относятся:

- задания на курсовое проектирование;

- экзаменационные вопросы;

Промежуточная аттестация в форме дифференцированного зачета проходит по результатам прохождения всех видов текущего контроля успеваемости.

3 ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

3.1 Задания и контрольные вопросы по лабораторным работам. Дисциплина «Проектирование открытых систем в защищенном исполнении» состоит из 5 разделов.

3.1.1 Задания по разделу: «Сущность, цели и задачи организации защиты информации открытых систем»:

- Основные положения современной теории защиты информации для открытых систем;

- Современные теории систем для организации и обеспечения функционирования открытых систем;

- Базовые подсистемы защиты информации и требования к ним.

3.1.2 Задания по разделу: «Основные принципы организации открытых систем в защищенном исполнении»:

- Факторы, оказывающие влияние на организацию защиты открытых систем;

- Функциональные и обеспечивающие подсистемы защиты информации;

- Требования, предъявляемые к сотрудникам, обеспечивающим функционирование открытых систем.

3.1.3 Задания по разделу: «Структура угроз для информационных ресурсов открытых систем»:

- Методы выявления состава защищаемых элементов. Объекты и субъекты защиты;

- Процедура выявления каналов несанкционированного доступа к информации в открытых системах;

- Особенности построения модели угроз для ИС. Нормативные документы, этапы создания;

- Структура типовой базовой модели угроз для ИС. Способы определения актуальных угроз безопасности.

3.1.4 Контрольные вопросы по разделу «Принципы криптографической защиты информации»:

- Нормативные документы ФСБ

- Понятие ЭЦП. Особенности использования

- Основные программные платформы, используемые в САПР

- Особенности контроля деятельности персонала, связанного с защитой информации

3.1.5 Контрольные вопросы по разделу «Аттестация средств защиты информации по требованиям безопасности»:

- Способы оценки эффективности принятых мер защиты в ИС. Анализ защищенности

- Эксплуатационная документация АС. Требования к ней, особенности эксплуатации

- Основные нормативные документы, регламентирующие создание и функционирование открытых систем в защищенном исполнении.

3.1.6 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

Вариант 1

Вопрос 1: «Технический канал утечки информации» в соответствии с НПА в ФСТЭК - это: 1) совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация; 2) совокупность средств доступа к информации, нарушающих правила разграничения доступа с использованием штатных средств; 3) совокупность физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация; 4) совокупность объекта технической разведки и средств, которыми добывается защищаемая информация.
Вопрос 2: Техническими каналами утечки информации, приводящими к возникновению угроз безопасности персональных данных, являются: 1) кражи технических средств информационной системы; 2) утечки акустической (речевой) информации; 3) утечки информации, реализуемые через общедоступные информационные сети; 4) утечки видовой информации; 5) утечки информации по каналам побочных электромагнитных излучений; 6) утечки информации, реализуемые через интернет.
Вопрос 3: «Защищаемые помещения» это помещения, специально предназначенные для: 1) хранения носителей конфиденциальной информации; 2) размещения технических средств информационной системы; 3) хранения носителей конфиденциальной информации и размещения технических средств информационной системы; 4) проведения конфиденциальных мероприятий.
Вопрос 4: «Обладатель информации» это: 1) лицо, самостоятельно создавшее информацию; 2) лицо, получившее на основании закона или договора право разрешать или ограничивать доступ к информации; 3) лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам; 4) лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.
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: Уровень защищенности ПДн для ИС, если в ней обрабатываются биометрические ПДн и актуальны угрозы второго типа, обрабатываются персональные данные сотрудников: 1) УЗ 1; 2) УЗ 2; 3) УЗ 3; 4) УЗ 4; 5) УЗ 5; 6) УЗ 6.
Вопрос 8: Документом, определяющим лицензируемые виды деятельности, является: 1) Постановление правительства РФ от 26 января 2006 г. № 45 «Об организации лицензирования отдельных видов деятельности»; 2) Постановление Правительства РФ от 15 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации»; 3) Постановление Правительства РФ от 31 августа 2006 г. № 532 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»; 4) Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»; 5) Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
Вопрос 9: Средства защиты от НСД какого класса по РД СВТ минимально достаточны для обеспечения любого уровня защищенности персональных данных: 1) 3; 2) 4; 3) 5; 4) 6.
Вопрос 10: Средствами защиты информации, подлежащими сертификации, являются: 1) Строительные материалы, используемые для отделки помещений в которых размещаются отдельные элементы ИСПДн; 2) Детали интерьера, используемые для размещения ИСПДн; 3) Средства контроля эффективности применения средств защиты информации; 4) Средства контроля эффективности прочности ограждений; 5) Средства защиты информации (технические, программные, программно-технические) от НСД, блокировки доступа и нарушения целостности.
Вопрос 11: Обязательной аттестации подлежат информационные системы следующих типов: 1) К 1 и К 2; 2) УЗ 1 и УЗ2 ; 3) К 1, К 2 и К 3; 4) К 2 и К 3; 5) Только УЗ 1; 6) Только К 2; 7) Только К 3; 8) ГИС.
Вопрос 12: Условием доработки функционирующих информационных систем является: 1) смена руководства организации; 2) смена администратора, ответственного за защиту информации;

3) изменение класса или уровня защищенности информационной системы; 4) изменение погодных условий.
Вопрос 13: 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 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: Основные требования к содержанию системы защиты персональных данных, при автоматизированной обработке, определяют следующие документы: 1) ФЗ 152; 2) ППРФ 1119; 3) ППРФ 687; 4) Приказ ФСТЭК №21; 5) Приказ ФСТЭК №31; 6) ФЗ 149.
Вопрос 16: «Специальные проверки» (спецпроверки) 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.
Вопрос 17: «Специальные исследования» 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.
Вопрос 18: «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 19: 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 20: Контроль состояния защиты информации отраслевыми и федеральными органами заключается в оценке соблюдения требований: 1) нормативно-методических документов по защите информации; 2) отраслевых стандартов; 3) работоспособности применяемых средств защиты информации в соответствии с их эксплуатационной документацией; 4) Трудового кодекса РФ; 5) знаний и выполнения персоналом своих функциональных обязанностей в части защиты информации.
Вопрос 21: Влияют ли угрозы недекларированных возможностей на уровень защищенности ИСПДн: a) Нет; b) Да, только для специального ПО; c) Да, для системного и прикладного ПО; d) Да, только для специальных категорий ПДн.
Вопрос 22: К средствам контроля защищенности информации от НСД относятся: 1) межсетевые экраны; 2) средства формирования и контроля полномочий доступа в информационных (автоматизированных) системах; 3) антивирусные средства; 4) сканеры безопасности.
Вопрос 23: 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 24: Сертификационные испытания СЗИ проводит: 1) ФСТЭК России; 2) испытательная лаборатория; 3) орган по сертификации; 4) заявитель самостоятельно.
Вопрос 25: Приказ ФСТЭК России, задающий требования к обеспечению безопасности персональных данных: 1)21; 2)17; 3)31; 4)378.
Вопрос 26: Количество уровней защищенности описанных в ПП 1119: 1)3; 2)4; 3)5; 4)6.
Вопрос 27: 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 28: Уровень защищенности ПДн для ИС, если в ней обрабатываются биометрические ПДн и актуальны угрозы второго типа, обрабатываются персональные данные сотрудников: 1) УЗ 1; 2) УЗ 2; 3) УЗ 3; 4) УЗ 4; 5) УЗ 5; 6) УЗ 6.
Вопрос 29: 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 30: Отключения электропитания относятся к угрозам: 1) естественным; 2) искусственным; 3) халатность персонала; 4) преднамеренные искусственные угрозы.

Вариант 2

Вопрос 1: Ошибка – это: 1) неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния 2) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций 3) негативное воздействие на программу
Вопрос 2: Отказ, ошибки, сбой – это: 1) случайные угрозы 2) преднамеренные угрозы 3) природные угрозы
Вопрос 3: Владелец информации это: 1) лицо, самостоятельно создавшее информацию; 2) лицо, получившее на основании закона или договора право разрешать или ограничивать доступ к информации; 3) лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам; 4) лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.
Вопрос 4: Сертификационные испытания СЗИ проводит: 1) ФСТЭК России; 2) испытательная лаборатория; 3) орган по сертификации; 4 заявитель самостоятельно.

Вопрос 5: Система защиты информации делится на:
1) ресурсы автоматизированных систем;
2) организационно-правовое обеспечение;
3) человеческий компонент.

Вопрос 6: Организация режима секретности в учреждениях и на предприятиях в РФ основывается на:
1) Гражданском кодексе РФ;
2) Конституции РФ;
3) требованиях федерального законодательства, касающегося вопросов государственной тайны, и соответствующих подзаконных актов Уголовном кодексе РФ.

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: Политика информационной безопасности (Security Policy) в организации определяет подход организации к управлению:
1) информационной безопасностью
2) технической безопасностью
3) технологической безопасностью
4) перечисленное в п.1-3

Вопрос 9: Для контроля защищенности информации применяются средства рекомендованные:
1) ФСТЭК России;
2) ФСБ России;
3) Роскомнадзором;
4) и прошедшие в установленном законом порядке процедуру оценки соответствия.

Вопрос 10: Основными функциями Федеральной службы по техническому и экспортному контролю являются:
1) организация и контроль за проведением работ по защите информации в органах государственного управления, объединениях, концернах, на предприятиях, в организациях и учреждениях от утечки по техническим каналам, от несанкционированного доступа к информации, обрабатываемой техническими средствами, и от специальных воздействий на информацию с целью ее уничтожения и искажения;
2) поддержание системы лицензирования деятельности предприятий, организаций и учреждений по осуществлению мероприятий и (или) оказанию услуг в области защиты информации и сертификации средств защиты информации проведение единой технической политики и координация работ по защите информации;
3) перечисленные в п. 1-3.

Вопрос 11: Под организационно-управленческой деятельностью в сфере информационной безопасности понимается:
1) организационное обеспечение информационной безопасности;
2) программное обеспечение информационной безопасности;
3) техническое обеспечение информационной безопасности;
4) технологическое обеспечение информационной безопасности.

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: Источник угрозы – это: 1) потенциальный злоумышленник; 2) злоумышленник; 3) природная среда.
Вопрос 14: Средствами защиты информации, подлежащими сертификации, являются: 1) Строительные материалы, используемые для отделки помещений в которых размещаются отдельные элементы ИСПДн; 2) Детали интерьера, используемые для размещения ИСПДн; 3) Средства контроля эффективности применения средств защиты информации; 4) Средства контроля эффективности прочности ограждений; 5) Средства защиты информации (технические, программные, программно-технические) от НСД, блокировки доступа и нарушения целостности.
Вопрос 15: Черви – это: 1) код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения; 2) код, обладающий способностью к распространению путем внедрения в другие программы; 3) программа действий над объектом или его свойствами.
Вопрос 16: Приказ ФСТЭК России, задающий требования к обеспечению безопасности персональных данных: 1)21; 2)17; 3)31; 4)378.
Вопрос 17: Отключения электропитания относятся к угрозам: 1) естественным; 2) искусственным; 3) халатность персонала; 4) преднамеренные искусственные угрозы.
Вопрос 18: Предпосылки появления угроз: 1) объективные 2) субъективные 3) преднамеренные
Вопрос 19: «Защищаемые помещения» это помещения: 1) специально предназначенные для хранения носителей конфиденциальной информации; 2) специально предназначенные для размещения технических средств информационной системы; 3) специально предназначенные для хранения носителей конфиденциальной информации и размещения технических средств информационной системы; 4) специально предназначенные для проведения конфиденциальных мероприятий.
Вопрос 20: Влияют ли угрозы недекларированных возможностей на уровень защищенности ИСПДн: 1) Нет; 2) Да, только для специального ПО; 3) Да, для системного и прикладного ПО; 4) Да, только для специальных категорий ПДн.

Вопрос 21: Отказ - это: 1) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций; 2) некоторая последовательность действий, необходимых для выполнения конкретного задания; 3) структура, определяющая последовательность выполнения и взаимосвязи процессов.
Вопрос 22: Расшифровывание злоумышленником сообщения, после его перехвата относят к угрозе: 1) зависящей от активности ИС; 2) не зависящей от активности ИС; 3) искусственной;
Вопрос 23: «Несанкционированный доступ к информации» это: 1) доступ, реализующий возможности совокупности физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация; 2) доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств; 3) доступ с использованием совокупности средств технической разведки и прочих средств, которыми добывается защищаемая информация; 4) доступ к информации, реализуемый путём уничтожения технических средств информационной системы.
Вопрос 24: СЗИ (система защиты информации) делится на: 1) ресурсы автоматизированных систем; 2) организационно-правовое обеспечение; 3) человеческий компонент.
Вопрос 25: К человеческому компоненту СЗИ относят: 1) системные порты; 2) администрация; 3) программное обеспечение.
Вопрос 26: Правовое обеспечение безопасности информации делится на: 1) международно-правовые нормы; 2) национально-правовые нормы; 3) государственные нормы.
Вопрос 27: К государственной тайне относят: 1) сведения, защищаемые государством в области военной, экономической … деятельности; 2) документированная информация; 3) сведения, получаемые в процессе профессиональной деятельности и службы.
Вопрос 28: Средства, используемые на инженерных и технических мероприятиях в защите информации: 1) аппаратные; 2) криптографические; 3) физические.
Вопрос 29: Конфиденциальная информация это: 1) которую нельзя передавать другим лицам; 2) документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации; 3) ограничение к источнику информации; 4) документ ограниченного пользования.

Вопрос 30: 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.

Вариант 3

Вопрос 1: Аудит информации – это: 1) аудиторская проверка; 2) накопление информации, а затем ее анализ; 3) действия направленные на проверку информации ее ценность, доступность и пригодность к применению; 4) это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически. Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.
Вопрос 2: Электронная цифровая подпись это: 1) документ, в котором информация представлена в электронно-цифровой Форме; 2) это подпись в виде цифр; 3) реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе; 4) это криптографическое преобразования информации с использованием закрытого ключа электронной цифровой подписи.
Вопрос 3: Уровень защищенности ПДн для ИС, если в ней обрабатываются биометрические ПДн и актуальны угрозы второго типа, обрабатываются персональные данные сотрудников равен: 1) УЗ 1; 2) УЗ 2; 3) УЗ 3; 4) УЗ 4; 5) УЗ 5; 6) УЗ 6.
Вопрос 4: Защита информации: 1)это комплекс мероприятий, направленных на обеспечение информационной безопасности. 2) это организационно-технические мероприятия; 3) ограничение допуска к информации; 4) сокращение числа лиц к информации.
Вопрос 5: Основой современной политики РФ в сфере информационной безопасности является: 1) Административный кодекс РФ;

2) Доктрина информационной безопасности РФ; 3) Конституция РФ; 4) Уголовный кодекс РФ.
Вопрос 6: Основой современной политики РФ в сфере информационной безопасности является: 1) Административный кодекс РФ; 2) Доктрина информационной безопасности РФ; 3) Конституция РФ; 4) Уголовный кодекс РФ.
Вопрос 7: Сертификационные испытания СЗИ проводит: 1) ФСТЭК России; 2) испытательная лаборатория; 3) орган по сертификации; 4) заявитель самостоятельно.
Вопрос 8: Риски информационной безопасности классифицируются на: 1) операционные риски; 2) потенциальные риски; 3) системные риски; 4) террористические риски.
Вопрос 9: К средствам контроля защищенности информации от НСД относятся: 1) межсетевые экраны; 2) средства формирования и контроля полномочий доступа в информационных (автоматизированных) системах; 3) антивирусные средства; 4) сканеры безопасности.
Вопрос 10: Программные средства – это: 1) специальные программы и системы защиты информации в информационных системах различного назначения; 2) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла; 3) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними.
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: Вредоносная программа - это: 1) программа, специально разработанная для нарушения нормального функционирования систем; 2) упорядочение абстракций, расположение их по уровням; 3) процесс разделения элементов абстракции, которые образуют ее структуру и поведение.

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 14: Информацию с ограниченным доступом делят на: 1) государственную тайну; 2) конфиденциальную информацию; 3) достоверную информацию.
Вопрос 15: Сбой – это: 1) такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент; 2) неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния; 3) объект-метод.
Вопрос 16: Присвоение чужого права относится к следующему виду угроз: 1) нарушение права собственности; 2) нарушение содержания; 3) внешняя среда.
Вопрос 17: Вирус – это: 1) код обладающий способностью к распространению путем внедрения в другие программы; 2) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов; 3) небольшая программа для выполнения определенной задачи.
Вопрос 18: Окно опасности – это: 1) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется; 2) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области; 3) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере.
Вопрос 19: Конфиденциальность – это: 1) защита от несанкционированного доступа к информации; 2) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов; 3) описание процедур.
Вопрос 20: Атака на информационную систему это: 1) попытка реализации угрозы; 2) потенциальная возможность определенным образом нарушить информационную безопасность; 3) программы, предназначенные для поиска необходимых программ.
Вопрос 21: Угроза безопасности это: 1) потенциальная возможность определенным образом нарушить информационную безопасность;

2) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных; 3) процесс определения отвечает на текущее состояние разработки требованиям данного этапа.
Вопрос 22: Основные составляющие информационной безопасности: 1) целостность 2) достоверность 3) конфиденциальность
Вопрос 23: Средства защиты от НСД какого класса по РД СВТ минимально достаточны для обеспечения любого уровня защищенности персональных данных: 1) 3; 2) 4; 3) 5; 4) 6.
Вопрос 24: Документом, определяющим лицензируемые виды деятельности, является: 1) Постановление правительства РФ от 26 января 2006 г. № 45 «Об организации лицензирования отдельных видов деятельности»; 2) Постановление Правительства РФ от 15 августа 2006 г. № 504 «О лицензировании деятельности по технической защите конфиденциальной информации»; 3) Постановление Правительства РФ от 31 августа 2006 г. № 532 «О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»; 4) Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»; 5) Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
Вопрос 25: Информационная безопасность зависит от: 1) компьютеров; 2) поддерживающей инфраструктуры; 3) информации.
Вопрос 26: Информационная безопасностью это: 1) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре; 2) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия; 3) отсутствие рисков в информационной системе.
Вопрос 27: К государственной тайне относят: 1) сведения, защищаемые государством в области военной, экономической … деятельности; 2) документированная информация; 3) сведения, получаемые в процессе профессиональной деятельности и службы.
Вопрос 28: «Обладатель информации» это: 1) лицо, самостоятельно создавшее информацию; 2) лицо, получившее на основании закона или договора право разрешать или ограничивать доступ к информации; 3) лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам; 4) лицо, самостоятельно создавшее информацию либо получившее право разрешать или

ограничивать доступ к информации, определяемой по каким-либо признакам.
Вопрос 29: СЗИ (система защиты информации) делится на: 1) ресурсы автоматизированных систем; 2) организационно-правовое обеспечение; 3) человеческий компонент.
Вопрос 30: 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.

3.3 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 дифференцированного зачета, экзамена и курсового проекта. Промежуточная аттестация в форме дифференцированного зачета проходит по результатам прохождения всех видов текущего контроля успеваемости.

4.2 Вопросы к экзамену:

1. Сущность, цели и задачи организации защиты информации.
2. Значение основных положений современной теории защиты информации для организации.
3. Значение современной теории систем для организации и обеспечения функционирования открытых систем.
4. Структура угроз для информационных ресурсов ОС.
5. Сущность, цели и задачи организации защиты информации.
6. Значение основных положений современной теории защиты информации для организации.
7. Значение современной теории систем для организации и обеспечения функционирования ОС.
8. Факторы, оказывающие влияние на организацию защиты ОС.
9. Основные принципы организации ОС.
10. Роль структуризации объекта в определении требований к защите
11. Основные группы требований к ОС.
12. Требования к защите применительно к различным защищаемым элементам ОС.
13. Факторы, определяющие состав защищаемой информации.
14. Основные этапы работы по выявлению состава защищаемой информации.

15. Управление рисками.
16. Методы выявления состава защищаемых элементов.
17. Какими факторами определяется состав угроз безопасности предприятия?
18. Какова процедура выявления каналов несанкционированного доступа к информации в ОС?
19. Чем определяется состав нарушителей и как осуществляется их категорирование?
20. Каким образом может проводиться оценка степени уязвимости информации в результате действий нарушителей различных категорий?
21. Какие компоненты входят в состав структуры ОС?
22. Какие критерии положены в основу классификации каждой группы средств, входящих в состав ОС?
23. Какие требования предъявляются к выбору методов и средств защиты при организации и функционировании ОС?
24. Как определяются условия функционирования ОС?
25. Определите значение моделирования объектов и процессов защиты ОС.
26. Какие компоненты входят в состав информационной модели ОС?
27. Каково общее содержание схемы технологического и организационного построения ОС?
28. Требования, предъявляемые к сотрудникам, обеспечивающим функционирование ОС.
29. Нормативные документы, регламентирующие деятельность и взаимодействие персонала с защищенной ОС.
30. Особенности контроля деятельности персонала, связанного с защитой информации.
31. Укажите стандарты (ГОСТ Р), применяемые при обеспечении информационной защиты ОС.

4.3 Критерии оценивания при промежуточной аттестации:

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

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

Оценка **“хорошо”** 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”** 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.

4.4 Задания на курсовую работу. Критерии и шкала оценивания по курсовой работе.

Курсовая работа по дисциплине состоит из двух частей:

Первая часть: Содержание и порядок выполнения работ на стадиях и этапах создания автоматизированных систем в защищённом исполнении.

Курсовая работа предполагает выполнение части этапов и освоение специфики части этапов создания информационных систем.

Формирование требований к системе ЗИ АСЗИ осуществляется на следующих стадиях создания АСЗИ, определенных ГОСТ 34.601:

- «Формирование требований к АС»;
- «Разработка концепции АС»;
- «Техническое задание».

На этапе 1 в общем случае проводят сбор данных об объекте автоматизации и осуществляемых видах деятельности;

- оценку качества функционирования объекта и осуществляемых видов деятельности, выявление проблем, решение которых возможно средствами автоматизации;
- оценку (технико-экономической, социальной и т.п.) целесообразности создания АС.

На этапе 2 проводят:

- подготовку исходных данных для формирования требований к РИС в защищенном исполнении на основе модели угроз и НПА (характеристика объекта автоматизации, описание требований к системе, ограничения допустимых затрат на разработку, ввод в действие и эксплуатацию, эффект, ожидаемый от системы, условия создания и функционирования системы);
- формулировку и оформление требований к безопасности АС.

На этапе 3 проводят оформление отчета о выполненных работах на данной стадии и оформление заявки на разработку РИС в защищенном исполнении (тактико-технического задания) или другого замещающего ее документа с аналогичным содержанием.

На этапах 1 и.2 организация-разработчик проводит детальное изучение объекта автоматизации и научно-исследовательские работы (при необходимости), связанные с

поиском путей и оценкой возможности реализации требований, оформляют и утверждают отчеты о НИР.

На этапе 3, в общем случае, проводят:

- разработку альтернативных вариантов концепции, создаваемой РИС в защищенном исполнении и планов их реализации;
- оценку необходимых ресурсов на их реализацию и обеспечение функционирования;
- оценку преимуществ и недостатков каждого варианта;
- сопоставление требований пользователя и характеристик предлагаемой системы;
- выбор оптимального варианта;
- определение порядка оценки качества и условий приемки системы;
- оценку эффектов, получаемых от системы.

На этапе 2.4 подготавливают и оформляют отчет, содержащий описание выполненных работ на стадии, описание и обоснование предлагаемого варианта концепции системы.

На этапе 3.1 проводят разработку, оформление, согласование и утверждение технического задания на автоматизированную систему (АС) и, при необходимости, - технических заданий на части АС.

Вторая часть: Проектирование системы ИБ

В качестве исходных данных студенты выбирают объект защиты в виде отдела, предприятия, либо фирмы, использующие в своей деятельности информационные системы, автоматизированные системы, веб-порталы и т.д.

Основываясь на результате выполнения лабораторных работ по дисциплине «Информационная безопасность автоматизированных информационных систем» было необходимо:

- проанализировать инфраструктуру выбранного предприятия;
- определить особенности существующих на предприятии автоматизированных информационных систем;
- проанализировать уязвимости АИС для конкретного предприятия;
- проанализировать угрозы на предприятии, использующих АИС;
- определить особенности построения и разработать прототип модели нарушителя с учетом атакующих воздействий на компоненты АИС;
- разработать прототип модели нарушителя;

− оценить эффективность средств защиты информации для данного предприятия и предложить средства для их усовершенствования.

На основании имеющихся в распоряжении исходных данных произвести оценку текущего уровня информационной безопасности и выработать рекомендации по совершенствованию системы защиты информации с приложением списка конкретных уязвимостей активного сетевого оборудования, серверов и др.

Примерное содержание основного раздела пояснительной записки.

Можно придерживаться следующей примерной формулировки глав основной части:

1. Общая характеристика объекта автоматизации.

1.1 Обследование инфраструктуры предприятия. Организационная структура предприятия.

1.2 Построение модели деятельности организации в методологии IDF0 («как есть» контекстная диаграмма).

1.3 Построение структурной диаграммы декомпозиции работы отдела.

Вывод по Главе 1 должен содержать оценку качества функционирования объекта и осуществляемых видов деятельности, выявление проблем, решение которых возможно средствами автоматизации; оценку целесообразности создания АС.

2. Формирование модели угроз и требований пользователя к АС.

2.1 Разработка актуальной модели угроз на предприятии.

2.2 Определение требований, компенсирующих угрозы в АС предприятия.

Вывод по Главе 2 должен содержать формулировку и оформление требований к безопасности АС на предприятии.

Глава 3 основной части курсового проекта должна содержать раскрытие этапов второй стадии процесса «Разработка концепции АС в защищенном исполнении»

3 Разработка альтернативных вариантов концепции создаваемой РИС в защищенном исполнении и планов их реализации

3.1 Создание диаграммы прецедентов (методология UML)

3.2 Создание диаграммы деятельности (методология UML)

3.3 Создание диаграммы взаимодействия объектов в виде диаграммы последовательности (методология UML)

Вывод по Главе 3 должен содержать оценку преимуществ и недостатков каждого варианта; сопоставление требований пользователя и характеристик предлагаемой системы; выбор оптимального варианта; оценку эффектов, получаемых от системы, содержащий

описание выполненных работ на этой стадии, описание и обоснование предлагаемого варианта концепции системы.

Глава 4 основной части курсового проекта должна содержать пример оформления технического задания по теме проектирования.

4 Разработка технического задания

В этой главе необходимо руководствоваться требованиями ГОСТ 34.602 – 89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.

Курсовой проект выполняется в виде пояснительной записки с приложением необходимых результатов моделирования. Курсовой проект должен содержать следующие структурные элементы:

- титульный лист;
- задание на курсовой проект
- содержание;
- введение;
- основная часть;
- заключение;
- список использованных источников;
- приложения (при необходимости).

Правила оформления курсового проекта должны соответствовать требованиям ГОСТ 7.32-2017.

В заключении в лаконичной форме подводятся итоги проделанной работы и делаются основные выводы по проекту.

Типовые задания на курсовой проект

Тема курсового проекта может формироваться индивидуально для студента с учетом особенностей конкретно взятого предприятия, организации, отдела, ресурса по следующему шаблону:

«Проектирование (модернизация) защищенной распределенной информационной системы (автоматизированной системы, веб-портала,…) для организации (указывается организация) на базе технологий (указывается технология защиты информации или конкретная реализация в виде наименования продукта по защите информации)».

Типовые технологии защиты информации:

1. Проектирование защищенной распределенной информационной системы для организации на базе технологий виртуальных частных сетей VPN.

2. Проектирование защищенной распределенной информационной системы для организации на базе технологий протоколов SSL,TSL ,IP sec, S-HTTP

3. Проектирование защищенной распределенной информационной системы для организации на базе технологий децентрализованного хранения данных сервера безопасности.

4. Проектирование защищенной распределенной информационной системы для организации базе технологий централизованного хранения данных сервера безопасности.

5. Проектирование защищенной распределенной информационной системы для организации на базе технологий протоколов TSL

6. Проектирование защищенной распределенной информационной системы для организации на базе технологий протоколов IP- sec

7. Проектирование защищенной распределенной информационной системы для организации на базе технологий протоколов S-HTTP

8. Проектирование защищенной распределенной информационной системы для организации на базе технологий протоколов SSL, SL

9. Проектирование защищенной распределенной информационной системы для организации на базе технологий децентрализованного хранения данных сервера безопасности. базе технологий протоколов SSL,TSL ,IP sec, S-HTTP

10. Проектирование защищенной распределенной информационной системы для организации на базе технологий децентрализованного хранения данных сервера безопасности. на базе технологий протоколов SSL, IP-sec, S-HTTP.

Критерии оценивания курсового проекта

Общее руководство и контроль за ходом выполнения курсового проекта осуществляется руководителем курсового проекта.

На время выполнения курсового проекта составляется расписание консультаций. В ходе консультации руководителем работы разъясняются назначение, задачи, структура и объём, принципы разработки и оформления, примерное распределение времени на выполнение отдельных частей курсового проекта, даются ответы на вопросы студентов.

Выполненный курсовой проект сдаётся студентом руководителю в установленный срок. Работа, не соответствующая предъявленным требованиям, возвращается студенту на

доработку. Защита курсового проекта является обязательной и проводится за счёт объёма времени, предусмотренного на изучение дисциплины, до начала экзаменационной сессии.

Во время защиты автору курсового проекта даётся возможность отстаивать и обосновывать свою точку зрения. Порядок обсуждения курсового проекта предусматривает ответы студента на вопросы руководителя курсового проекта. По итогам защиты выставляется оценка за курсовой проект.

Максимальный балл за курсовую работу выставляется в том случае, если студент полностью выполнил все части задания на курсовой проект. Проанализировал угрозы и уязвимости системы, предложил решения по повышению эффективности системы защиты и оценил эффективность предложенных решений. Студент грамотно подготовил пояснительную записку, ответил на все вопросы преподавателя.

Средний балл за курсовую работу выставляется в том случае, если студент полностью выполнил все части задания на курсовую работу, но выполнил некоторые задания частично (степень выполнения не менее 70%), и защитил свою работу преподавателю, ответив не менее чем на 70% его вопросов.

Минимальный балл за курсовую работу выставляется в том случае, если студент полностью выполнил все задания своего варианта, но смог ответить на 50% вопросов преподавателя и продемонстрировал минимум знаний в области анализа угроз безопасности и проектирования систем безопасности для ИС в защищенном исполнении. Либо, студент выполнил задание частично, и защитил свою работу преподавателю, ответив на более чем 50% вопросов.

Балл за курсовую работу не выставляется, если студент полностью или частично выполнил задания своего варианта, но не ответил на вопросы преподавателя и не продемонстрировал практических умений.

СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

Фонд оценочных средств для аттестации по дисциплине «Проектирование открытых систем в защищенном исполнении» 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 (протокол № 7 от 20.04.2022 г.)

Заведующая кафедрой  Н.Я.Великите