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)

«ЗАЩИТА ИНФОРМАЦИИ»

основной профессиональной образовательной программы бакалавриата по направлению подготовки

09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

Профиль программы

«АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ ОБРАБОТКИ ИНФОРМАЦИИ И УПРАВЛЕНИЯ»

ИНСТИТУТ цифровых технологий

РАЗРАБОТЧИК Кафедра систем управления и вычислительной техники

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-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1: Использует принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Защита информации	*Знать:* виды угроз ИС и методы обеспечения информационной безопасности, основные понятия и определения в области защиты информации; - концепции и методы защиты информации; - источники, риски и формы атак на информацию; стратегии аутентификации и авторизации; - концепции сетевого аудита; технологии обнаружения вторжения; - стратегии политик безопасности; принципы сетевой обороны. *Уметь* выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС, анализировать угрозы и факторы, влияющие на безопасность информации в компьютере, компьютерной системе и сети; - создавать план защиты информационных объектов и их информационного взаимодействия; выбирать и применять обоснованное средство защиты; - обновлять систему безопасности с использованием служб обновления, планировать политику безопасности объекта информатизации. *Владеть:* методами управления проектами ИС и защиты информации, конфигурированием параметров безопасности подключения системы к Интернет; - использованием средств защиты файлов шифрованием; - конфигурированием параметров аутентификации и авторизации; - администрированием средств защиты информации; - планированием защиты компьютерной сети.

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 Защитаинформации изучается 1 семестр и состоит из 5 разделов.

3.1.1 Задания по разделу: «Организация информационной защиты»:

- Требования к защите информации. Концепции многоуровневой информационной защитысистемы. Структура систем защиты АСОИУ;
- Основные определения и классификации угроз.

3.1.2 Задания по разделу: «Защита доступа к информационным ресурсам»:

- Стандартные и специальные права доступа;
- Управление правами доступа пользователей/групп к информационным ресурсам;
- Базовая стратегия использования групп. Матрица доступа.

3.1.3 Задания по разделу: «Основы криптографической защиты данных»:

- Блочные и потоковые криптосистемы;
- Криптосистемы с открытым ключом;
- Методы и средства хранения и распределения ключей. Определения и классификациякриптопротоколов.

3.1.4 Контрольные вопросы по разделу «Безопасность удаленного доступа и межсетевого взаимодействия»:

- Угрозы сетевым компонентам на уровнях модели OSI
- Способы защиты информации в сетях. Протоколы защиты информации в сетях
- Классификация сетевых атак. Межсетевые экраны

3.1.5 Контрольные вопросы по разделу «**Защита системы от вредоносных программ**»:

- Виды антивирусных программ Способы обнаружения и защиты
- Защита программ от изменения и контроль целостности. Методы защиты от спама.

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: Информационная безопасность 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 2: Защита информации – это: 1) комплекс мероприятий, направленных на обеспечение информационной безопасности; 2) процесс разработки структуры базы данных в соответствии с требованиями пользователей; 3) небольшая программа для выполнения определенной задачи.
Вопрос 3: Информационная безопасность зависит от: 1) компьютеров; 2) поддерживающей инфраструктуры; 3) информации.
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) 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: Основные составляющие информационной безопасности:
1) целостность;
2) достоверность;
3) конфиденциальность.

Вопрос 8: События, произошедшие во время существования окна опасности:
1) должно стать известно о средствах использования пробелов в защите;
2) должны быть выпущены соответствующие заплаты;
3) заплаты должны быть установлены в защищаемой И.С.

Вопрос 9: Угрозы можно классифицировать по нескольким критериям:
1) по спектру И.Б.;
2) по способу осуществления;
3) по компонентам И.С.

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: 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 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: 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 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: 1) Нет; 2) Да, только для специального ПО; 3) Да, для системного и прикладного ПО; 4) 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: 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 29: 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 30: Отключения электропитания относятся к угрозам:
1) естественным;
2) искусственным;
3) халатность персонала;
4) преднамеренные искусственные угрозы.

Вариант 2

Вопрос 1: 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 2: 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 3: «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 4: Сертификационные испытания СЗИ проводит:
1) ФСТЭК России;
2) испытательная лаборатория;
3) орган по сертификации;
4) заявитель самостоятельно.

Вопрос 5: 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 6: Присвоение чужого права относится к следующему виду угроз:
1) нарушение права собственности;
2) нарушение содержания;
3) внешняя среда.

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: Сбой – это:
1) такое нарушение работоспособности какого-либо элемента системы вследствие чего функции выполняются неправильно в заданный момент;
2) неправильное выполнение элементом одной или нескольких функций происходящее вследствие специфического состояния;
3) объект-метод.

Вопрос 9: К человеческому компоненту СЗИ относится:
1) системные порты;
2) администрация;
3) программное обеспечение.

Вопрос 10: Правовое обеспечение безопасности информации – это:
1) совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации;
2) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных;
3) организационные меры безопасности.

Вопрос 11: «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 12: Информацию с ограниченным доступом делят на:
1) государственную тайну;
2) конфиденциальную информацию;
3) достоверную информацию.

Вопрос 13: 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 14: 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 15: К организационно - административному обеспечению информации относится:
1) взаимоотношения исполнителей;
2) подбор персонала;
3) регламентация производственной деятельности.

Вопрос 16: 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 17: Риски информационной безопасности классифицируются на:
1) операционные риски
2) потенциальные риски
3) системные риски
4) террористические риски

Вопрос 18: 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 19: Виды негативных воздействий на информационные активы, защиту от которых предполагает информационная безопасность:
1) нарушение конфиденциальности информации;
2) недоступность информационных ресурсов;
3) разрушение (утеря, необратимое изменение) информации;
4) перечисленные в п. 1-3.

Вопрос 20: Основной задачей организационной работы в сфере информационной безопасности является:

1) обеспечение комплексности всех решений, реализуемых в процессе обеспечения информационной безопасности;
2) обеспечение непрерывности и целостности процессов информационной безопасности;
3) управление человеческими ресурсами и поведением персонала с учетом необходимости решения задач информационной безопасности;
4) перечисленные в п. 1-3

Вопрос 21: Основные задачи и функции государственных органов РФ в сфере информационной безопасности связаны с:

1) защитой информации, имеющей государственную важность;
2) охраной общественных интересов;
3) предотвращением противоправной деятельности;
4) перечисленными в п. 1-3.

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: 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 24: Криптографические средства – это:

1) средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования;
2) специальные программы и системы защиты информации в информационных системах различного назначения;
3) механизм, позволяющий получить новый класс на основе существующего

Вопрос 25: 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 26: 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 27: 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 28: 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 29: 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 автоматическимреагированием на выявленные нештатные ситуации называется активным

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: Биометрия это:
1) представляет собой совокупность автоматизированных методов;
2) идентификации и/или аутентификации людей на основе их физиологических и поведенческих характеристик;
3) все то, что имеет признак отличия в антропометрии;
4) биометрический шаблон;
5) новое направление в криптографии.

Вопрос 2: Целью мероприятий в области информационной безопасности являются:
1) мероприятия по защите информации;
2) защита интересы субъектов информационных отношений;
3) организация противодействия перехвата информации;
4) накопление опыта противодействия в информационной борьбе.

Вопрос 3: 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 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: Средства, используемые на инженерных и технических мероприятиях в защите информации: 1) аппаратные; 2) криптографические; 3) физические.
Вопрос 6: 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 7: Правовое обеспечение безопасности информации делится на: 1) международно-правовые нормы; 2) национально-правовые нормы; 3) государственные нормы.
Вопрос 8: К человеческому компоненту СЗИ относят: 1) системные порты; 2) администрация; 3) программное обеспечение.
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: СЗИ (система защиты информации) делится на: 1) ресурсы автоматизированных систем; 2) организационно-правовое обеспечение; 3) человеческий компонент.
Вопрос 11: Побочное влияние – это: 1) негативное воздействие на систему в целом или отдельные элементы; 2) нарушение работоспособности какого-либо элемента системы вследствие чего функции выполняются неправильно в заданный момент; 3) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций.
Вопрос 12: 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 13: Предпосылки появления угроз: 1) объективные; 2) субъективные; 3) преднамеренные.
Вопрос 14: 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 15: Основными источниками внутренних отказов являются: 1) ошибки при конфигурировании системы; 2) отказы программного или аппаратного обеспечения; 3) выход системы из штатного режима эксплуатации.
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: Основные требования к содержанию системы защиты государственных ИС, при автоматизированной обработке, определяют следующие документы: 1) ФЗ 152; 2) ППРФ 1119; 3) ППРФ 687; 4) Приказ ФСТЭК №17; 5) Приказ ФСТЭК №31; 6) ФЗ 149.
Вопрос 18: Источник угрозы – это: 1) потенциальный злоумышленник; 2) злоумышленник; 3) природная среда.
Вопрос 19: Целостность можно подразделить на: 1) статическую; 2) динамичную; 3) структурную.
Вопрос 20: 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 21: 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 22: 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 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: 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;
4) Уголовном кодексе РФ.

Вопрос 25: 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 26: Система защиты информации делится на:
1) ресурсы автоматизированных систем;
2) организационно-правовое обеспечение;
3) человеческий компонент.

Вопрос 27: Информация в информационной системе 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 28: 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 29: Отказ, ошибки, сбой – это: 1) случайные угрозы 2) преднамеренные угрозы 3) природные угрозы
Вопрос 30: 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

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 экзамена.

Вопросы к экзамену:

1. Роль информации в современном мире
2. Значение защиты
3. Аспекты защиты. Анализ схем защиты
4. Современная система удостоверяющих документов и её недостатки
5. Бесперспективность защиты носителей. Практика выявления поддельных документов
6. Организация защиты информации в вычислительном центре (ВЦ) крупного предприятия.Внешнее окружение ВЦ
7. Способы контроля доступа к информации.
8. Применимость мер защиты. Надежность и восстановление ЭВМ
9. Экономические проблемы ЗИ.
10. Меры противодействия и затраты на их организацию
11. Понятия, относящиеся к защите ВС. Целостность ресурсов, защита ресурсов, право владения, надежность.
12. Защита вычислительной сети. Классификация вторжений.

13. Концепция защищенной ВС.
14. Защита объектов ВС.
15. Защита линий связи.
16. Защита баз данных.
17. Защита подсистемы управления ВС.
18. Классификация сбоев и нарушения прав доступа к информации.
19. Физическая защита кабельной системы.
20. Физическая защита систем электроснабжения.
21. Системы архивирования и дублирования информации.
22. Защита информации в операционных системах.
23. Защита информации в прикладном ПО.
24. Способы идентификации пользователей.
25. Основные механизмы проверки подлинности пароля.
26. Механизм проверки подлинности "рукопожатие".
27. Проблема защиты информации в распределенных сетях.
28. Брандмауеры. Основные понятия.
29. Межсетевой экран. Классификация межсетевых экранов.
30. Классификация компьютерных вирусов
31. Структура файловых, резидентных вирусов и вирусов-червей
32. Жизненный цикл компьютерных вирусов
33. Способы и симптомы заражения вирусами
34. Общая классификация средств защиты от вирусов
35. Стандарт шифрования данных DES
36. Асимметрические (открытые) криптосистемы
37. Применение криптографии.
38. Основные направления компьютерных преступлений

4.2 Критерии оценивания при промежуточной аттестации:

Оценка **“отлично”** на зачете 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.

5 СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

Фонд оценочных средств для аттестации по дисциплине «Защита информации» представляет собой компонент основной профессиональной образовательной программы образовательной программы бакалавриата по направлению подготовки 09.03.01 Информатика и вычислительная техника, профиль «Автоматизированные системы обработки информации и управления».

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

Заведующая кафедрой  Н.Я. Великите

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры систем управления и вычислительной техники 25.04.2022 г. (протокол № 5).

Заведующий кафедрой  В.А. Петрикин