СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Факультет ***Математики и информационных технологий***
Кафедра ***Математического моделирования***

Оценочные материалы по дисциплине (модулю)

дисциплина ***Организационное и правовое обеспечение информационной безопасности***

Блок Б1, обязательная часть, Б1.О.27
цикл дисциплины и его часть (обязательная часть или часть, формируемая участниками образовательных отношений)

Направление

10.03.01	***Информационная безопасность***
код	наименование направления

Программа

Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения

Очно-заочная

Для поступивших на обучение в
2023 г.

Разработчик (составитель)
к. ф.-м. н., доцент
Гнатенко Ю. А.
ученая степень, должность, ФИО

Стерлитамак 2023

1. Перечень компетенций, индикаторов достижения компетенций и описание показателей и критериев оценивания результатов обучения по дисциплине (модулю)

Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине (модулю)	Показатели и критерии оценивания результатов обучения по дисциплине (модулю)				Вид оценочного средства
1	2	3	4				5
			неуд.	удовл.	хорошо	отлично	
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации,	ОПК-6.2. определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	Обучающийся должен: меры по обеспечению информационной безопасности и методы управления процессом их реализации на объекте защиты.	Отсутствие знаний	Неполные представления об информационных ресурсах, подлежащих защите, и возможных путях реализации защиты	Сформированные, но содержащие отдельные пробелы представления об информационных ресурсах, подлежащих защите, и возможных путях реализации защиты на основе анализа структуры и содержания информационных процессов и особенностей	Сформированные систематические представления об информационных ресурсах, подлежащих защите, и возможных путях реализации защиты на основе анализа структуры и содержания информационных процессов и особенностей	тест

Федеральной службы по техническому и экспортному контролю;					процессов и особенностей функционирования объекта защиты	функционирования объекта защиты	
	ОПК-6.3. использовать нормативные правовые акты в профессиональной деятельности	Обучающийся должен: знать угрозы безопасности информации и возможные пути их реализации, нормативные правовые акты, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.	Отсутствие знаний	Неполные представления о нормативных правовых актах в профессиональной деятельности	Сформированные, но содержащие отдельные пробелы представления о нормативных правовых актах в профессиональной деятельности	Сформированные систематические представления о нормативных правовых актах в профессиональной деятельности	тест
	ОПК-6.1. принимать участие в	Обучающийся должен: владеть навыками	Отсутствие знаний	Неполные представления об организации и	Сформированные, но содержащие	Сформированные систематические	тест

	организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	применения нормативных правовых актов, нормативных и методических документов, регламентирующие деятельность по защите информации в организации.		проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	отдельные пробелы представления об организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	представления об организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	
ОПК-5. Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере	ОПК-5.3. Наделен навыками применения нормативных правовых актов, нормативных и методических документов, регламентирующие деятельность по защите информации в	Обучающийся должен: знать основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения	Отсутствие навыков	В целом успешное, но непоследовательное владение нормативными правовыми актами в профессиональной деятельности	В целом успешное, но содержащее отдельные пробелы владения нормативными правовыми актами в профессиональной деятельности	Успешное и последовательное владение нормативными правовыми актами в профессиональной деятельности	тест

профессиональной деятельности;	организации.	информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации					
	ОПК-5.2. Понимает и определяет необходимые нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации.	Обучающийся должен: уметь применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности.	Отсутствие умений	В целом успешное, но не систематическое применение нормативных правовых актов в профессиональной деятельности	В целом успешное, но содержащее отдельные пробелы применения нормативных правовых актов в профессиональной деятельности	Сформированное умение применять нормативные правовые акты в профессиональной деятельности	тест
	ОПК-5.1. Знает нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность	Обучающийся должен: владеть навыками работы с нормативными правовыми актами; навыками организации и	Отсутствие знаний	Неполные представления о нормативных правовых актах в профессиональной деятельности	Сформированные, но содержащие отдельные пробелы представления о нормативных правовых актах в	Сформированные систематические представления о нормативных правовых актах в профессиональной	тест

	по защите информации в организации.	обеспечения режима секретности			профессиональной деятельности	деятельности	

2. Оценочные средства, необходимые для оценки результатов обучения по дисциплине (модулю)

Тесты

Перечень заданий для оценки уровня сформированности компетенции ОПК-5 (индикатор достижения компетенции ОПК-5.1)

1. Что такое политика информационной безопасности
   а) Методология защиты информации
   б) Идеология информационной безопасности
   в) Концепция защиты информации
   г) Система официальных взглядов на место государства в современном мире информационных технологий

2. Какой федеральный закон считается рамочным по защите информации?
   а) ФЗ «О коммерческой тайне»
   б) ФЗ «О персональных данных»
   в) ФЗ «Об информации, информационных технологиях и о защите информации»
   г) ФЗ «О государственной тайне»

3. Номер ФЗ «Об информации, информационных технологиях и о защите информации»является:
   а) 188 ФЗ
   б) 152 ФЗ
   в) 149 ФЗ
   г) 214 ФЗ

4. Лицензирование деятельности по распространению криптографических средств,осуществляет:
   а) ФСБ
   б) ФСТЭК
   в) Роскомнадзор
   г) Ростехнадзор

5. Подключение ИС, обрабатывающих служебную тайну к сети Интернет:
   а) допускается
   б) не допускается
   в) допускается только с использованием специально предназначенных для этогосредств
   г) допускается только с использованием средств защиты известных производителей

6. Специальная проверка это
   а) выявление возможных каналов утечки информации Российскими техническимисредствами
   б) определение соответствия условий эксплуатации ОИ требованиям аттестатовсоответствия объектам защиты

в) проверки технических средств на наличие возможно внедренных электронныхустройств перехвата информации

г) контроль надежности работы оборудования информационной системы

7. Каким документов определяются права человека на доступ к информации?

а) Доктриной ИБ

б) Конституцией

в) ФЗ «О коммерческой тайне»

г) Стратегия национальной безопасности

8. Источниками угроз несанкционированного доступа являются:

1. **нарушители**
2. природные факторы
3. **носители вредоносных программ**
4. **аппаратные закладки**
5. отказы оборудования
6. отказы программного обеспечения

а) 126

б) 134

в) 256

г) 135

9. Основные направления обеспечения информационной безопасности указанные в Доктрине ИБ

1. стратегическое развитие военных конфликтов, которые могут возникнуть врезультате применения информационных технологий
2. совершенствование Вооруженных Сил Российской Федерации
3. **прогнозирование, обнаружение и оценка информационных угроз, включаяугрозы Вооруженным Силам Российской Федерации в информационной сфере**
4. **содействие обеспечению защиты интересов союзников Российской Федерации винформационной сфере**

а) 14

б) 34

в) 23

г) 24

10. Документом, определяющим лицензируемые виды деятельности, является:

а) Постановление правительства РФ от 26 января 2006 г. № 45 Об организациилицензирования отдельных видов деятельности

б) Постановление Правительство РФ от 15 августа 2006 г. № 504 О лицензированиидеятельности по технической защите конфиденциальной информации

в) Постановление Правительства РФ от 31 августа 2006 г. № 532 О лицензированиидеятельности по разработке и (или) производству средств защиты конфиденциальнойинформации

г) ФЗ «О лицензировании отдельных видов деятельности» 99-ФЗ от 4 мая 2011 г.

11. Средствами защиты информации, подлежащими сертификации являются:
1. строительные материалы, используемые для отделки помещений в которыхразмещаются 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**

а) 23
б) 12
в) 35
г) 45

12. Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:
1. **противодействие использованию информационных технологий для пропагандыэкстремистской идеологии, распространения ксенофобии, идей национальнойисключительности в целях подрыва суверенитета, политической и социальнойстабильности, насильственного изменения конституционного строя, нарушениятерриториальной целостности Российской Федерации**
2. осуществление контроля за населением РФ с использованием техническихсредств и информационных технологий специальными службами и организациямииностранных государств, а также отдельными лицами
3. **повышение защищенности критической информационной инфраструктуры иустойчивости ее функционирования, развитие механизмов обнаружения ипредупреждения информационных угроз и ликвидации последствий их проявления,повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций,вызванных информационно-техническим воздействием на объекты критическойинформационной инфраструктуры**
4. допущения иностранного контроля за функционированием объектовинформатизации, на территории Российской Федерации

а) 12
б) 23
в) 34
г) 13

13. «Информационная система» это:
а) совокупность информации, информационных технологий и технических средств
б) совокупность информации, информационных технологий, технических средств иперсонала, обслуживающего систему
в) совокупность информационных технологий и технических средств

г) совокупность информации, технических средств и персонала, обслуживающегоинформационную систему
д) совокупность информации, технических средств и персонала, обслуживающегои эксплуатирующего информационную систему

14. Количество категорий внутренних нарушителей для ИСПДн, определяемых нормативными документами ФСТЭК:
а) 4
б) 5
в) 6
г) 8

15. Основными элементами ИС являются:
1. помещения для размещения технических средств
2. **персональные данные, содержащиеся в базах данных**
3. контролируемая зона
4. **информационные технологии**
5. обслуживающий персонал
6. **технические средства обработки информации**
7. ограждающие конструкции
8. технические средства перевозки материальных носителей информации

а) 135
б) 246
в) 378
г) 468

Перечень заданий для оценки уровня сформированности компетенции ОПК-6 (индикатор достижения компетенции ОПК-6.1)

16. К каким мерам защиты относится политика безопасности?
а) к административным
б) к законодательным
в) к программно-техническим
г) к процедурным

17. Для защиты объектов авторского права от нарушения пользователем условий предоставления лицензии предназначены меры защиты информации, относящиеся к категории
а) Административных
б) Криптографических
в) Технических
г) Стеганографических

18. Как называется свойство информации, означающее отсутствиенеправомочных, и не предусмотренных ее владельцем изменений?
а) целостность

б) доступность
в) конфиденциальность
г) аутентичность

19. К основным принципам построения системы защиты АИС относятся:
а) открытость
б) взаимозаменяемость подсистем защиты
в) минимизация привилегий
г) комплексность

20. Диспетчер доступа...
а) использует базу данных защиты, в которой хранятся правиларазграничения доступа
б) использует атрибутные схемы для представления матрицы доступа
в) выступает посредником при всех обращениях субъектов к объектам
г) фиксирует информацию о попытках доступа в системном журнале

21. Какие предположения включает неформальная модельнарушителя?
а) о возможностях нарушителя
б) о категориях лиц, к которым может принадлежать нарушитель
в) о предыдущих атаках, осуществленных нарушителем
г) об уровне знаний нарушителя

22. Что представляет собой доктрина информационной безопасностиРФ?
а) нормативно-правовой акт, устанавливающий ответственность заправонарушения в сфере информационной безопасности
б) **федеральный закон, регулирующий правоотношения в области**информационной безопасности
в) целевая программа развития системы информационной безопасностиРФ, представляющая собой последовательность стадий и этапов
г) совокупность официальных взглядов на цели, задачи, принципы иосновные направления обеспечения информационной безопасности РоссийскойФедерации

23. К какому виду мер защиты информации относится утвержденнаяпрограмма работ в области безопасности?
а) политика безопасности верхнего уровня
б) политика безопасности среднего уровня
в) политика безопасности нижнего уровня
г) принцип минимизации привилегий

24. Чтобы подписать сообщение электронной цифровой подписью,используются:
а) открытый ключ отправителя
б) открытый ключ получателя
в) закрытый ключ отправителя
г) закрытый ключ получателя

25. Создание и использование средств опасного воздействия наинформационные сферы других стран мира и нарушение нормальногофункционирования информационных и телекоммуникационных системэто....

а) информационная война
б) информационное оружие
в) информационное превосходство
г) холодная война

26. Информация не являющаяся общедоступной, которая ставит лиц,обладающих ею в силу своего служебного положения в преимущественноеположение по сравнению с другими объектами.

а) служебная информация
б) коммерческая тайна
в) банковская тайна
г) конфиденциальная информация

27. Гарантия того, что конкретная информация доступна только томукругу лиц, для которых она предназначена

а) конфиденциальность
б) целостность
в) доступность
г) аутентичность

28. Гарантия того, что АС ведет себя в нормальном и внештатном режиметак, как запланировано

а) надежность
б) контролируемость
в) устойчивость
г) доступность

29. Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это...

а) комплексное обеспечение ИБ
б) безопасность АС
в) угроза ИБ
г) политика безопасности

30. Некоторое секретное количество информации, известное толькопользователю и парольной системе, которое может быть запомненопользователем и предъявлено для прохождения процедурыутентификации это ....

а) идентификатор пользователя
б) пароль пользователя
в) учетная запись пользователя
г) парольная система

31. К принципам информационной безопасности относятся

1. Скрытость
2. Масштабность

3. **Системность**
4. **Законность**
5. **открытости алгоритмов**

а) 134
б) 245
в) 123
г) 345

32. Охрана персональных данных, государственной служебной и другихвидов информации ограниченного доступа это...

а) Защита информации
б) Компьютерная безопасность
в) Защищенность информации
г) Безопасность данных

Перечень заданий для оценки уровня сформированности компетенции ОПК-5 (индикатор достижения компетенции ОПК-5.2)

33. Набор аппаратных и программных средств для обеспечениясохранности, доступности и конфиденциальности данных:

а) Защита информации
б) Компьютерная безопасность
в) Защищенность информации
г) Безопасность данных

34. Средства уничтожения, искажения или хищения информационныхмассивов, добывания из них необходимой информации послепреодоления систем защиты, ограничения или воспрещения доступа кним это:

а) информационная война
б) информационное оружие
в) информационное превосходство
г) холодная война

35. Информация позволяющая ее обладателю при существующих иливозможных обстоятельствах увеличивать доходы, сохранить положение нарынке товаров, работ или услуг это:

а) государственная тайна
б) коммерческая тайна
в) банковская тайна
г) конфиденциальная информация

36. Гарантия того, что при хранении или передаче информации не былопроизведено несанкционированных изменений:

а) конфиденциальность
б) целостность

в) доступность
г) аутентичность

37. Уровень защиты, при котором затраты, риск, размер возможногоущерба были бы приемлемыми:
а) принцип системности
б) принцип комплексности
в) принцип разумной достаточности
г) принцип гибкости системы

38. Совокупность норм, правил и практических рекомендаций,регламентирующих работу средств защиты АС от заданного множестваугроз безопасности:
а) Комплексное обеспечение информационной безопасности
б) Безопасность АС
в) атака на автоматизированную систему
г) политика безопасности

39. Особенностями информационного оружия являются:
1. Системность
2. Открытость
3. **Универсальность**
4. **Скрытность**

а) 34
б) 24
в) 13
г) 14

40. К функциям информационной безопасности относятся:
а) выявление источников внутренних и внешних угроз
б) защита государственных информационных ресурсов
в) подготовка специалистов по обеспечению информационной безопасности
г) все ответы верны

41. К типам угроз безопасности парольных систем относятся
а) словарная атака
б) тотальный перебор
в) разглашение параметров учетной записи
г) все варианты ответа верны

42. К нацональным интересам РФ в информационной сфере относятся:
а) Реализация конституционных прав на доступ к информации
б) Защита информации, обеспечивающей личную безопасность
в) Защита независимости, суверенитета, государственной и территориальнойцелостности
г) Сохранение и оздоровлении окружающей среды

43. По принципу действия меры защиты информации подразделяются на:

а) Законодательные, морально-этические, административные, организационно-технические, программно-технические
б) Законодательные, морально-этические, административные, организационные, программно-технические
в) Организационные, криптографические, меры технической ЗИ, стенографические
г) Законодательные, морально-этические, административные, организационно-технические

44.Укажите все задачи, для решения которых организационные меры ЗИ могут рассматриваться как эффективные:
1. Защита от нарушителей, действующих из любопытства
2. **Снижение вероятности угроз, вызванных поломками оборудования объекта информатизации**
3. **Защита от нарушителей, входящих в персонал объекта информатизации**
4. **Защита от перехвата информации, передаваемой по открытым каналам связи**

а) 123
б) 134
в) 124
г) 234

45. Права и обязанности участников информационных отношений устанавливают
а) Административные меры ЗИ
б) Организационные меры ЗИ
в) Административно-правовые меры ЗИ
г) технические меры ЗИ

46. Укажите все мероприятия, предусматриваемые в рамках административных мер защиты информации:
1. **Управление персоналом**
2. **Разработка политики безопасности организации**
3. Контроль доступа на территорию объекта информатизации
4. **Управление рисками**

а) 123
б) 134
в) 124
г) 234

47. Совокупность людей, процедур и оборудования, защищающих объект информатизации от действий, нарушающих его безопасность представляет собой
а) Систему комплексной защиты
б) Организационно-технические меры защиты
в) Программно-технический комплекс защиты
г) Систему физической защиты

48. Программно-технические средства защиты информации

а) Обеспечивают контроль доступа физических лиц на территорию объекта информатизации
б) Принципиально разграничивают санкционированных пользователей и прочих субъектов
в) Снижают вероятность нарушений безопасности информации из-за повреждений автоматизированной системы
г) Устанавливают порядок доступа к информации и работы с ней в пределах

Перечень заданий для оценки уровня сформированности компетенции ОПК-6 (индикатор достижения компетенции ОПК-6.2)

49. Установите верное соответствие видов информации с их содержательным определением

А. Документированная информация
Б. Электронный документ
В. Данные

1. информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека
2. зафиксированная на материальном носителе путем документирования информация с определенными реквизитами
3. документированная информация, представленная в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин.

а) А3, Б2, В1
б) А2, Б3, В1
в) А1, Б2, В3
г) А1, Б3, В2

50. Переводчик, согласно федеральному закону «Об информации, информационных технологиях и о защите информации», при отсутствии иных условий, может рассматриваться в качестве обладателя

а) Текста переводимого им произведения
б) Используемого им в работе словаря
в) Созданного им перевода текста
г) Документа с замечаниями редактора к созданному переводу

51. Предоставление информации отличается от распространения информации, согласно федеральному закону «Об информации, информационных технологиях и о защите информации»

а) Характером лица или круга лиц, осуществляющего получение информации
б) Стороной, являющейся инициатором действий
в) Формой представления передаваемой информации
г) Конфиденциальностью передаваемой информации

52. Укажите все ситуации, которые, согласно федеральному закону «Об информации, информационных технологиях и о защите информации», можно рассматривать как распространение информации (несколько вариантов):

1. Публикация статьи в средствах массовой информации

2. Рассылка внутреннего регламента сотрудникам организации на основе штатного расписания по корпоративной почте
3. **Размещение бумажного объявления на доске объявлений**
4. Демонстрация презентации на совещании руководителей отделов
5. Демонстрация учебного видео на уроке в школе
6. **Размещение записи на странице в социальной сети**

а) 245
б) 236
в) 136
г) 135

53. Согласно федеральному закону «Об информации, информационных технологиях и о защите информации», электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия:

а) Человеком с использованием электронных вычислительных машин
б) Техническими средствами информационных систем
в) Программным обеспечением информационных систем
г) Программным обеспечением систем обработки информации

54. Защищаемая информация, согласно ГОСТ «Защита информации. Основные термины и определения» - это подлежащая защите информация,

а) Не являющаяся общеизвестной
б) Представляющая ценность для ее обладателя
в) Являющаяся предметом собственности
г) Относящаяся к установленной законом категории

55. Укажите все варианты того, что может являться объектом защиты информации, предусмотренные ГОСТ «Защита информации. Основные термины и определения» (несколько вариантов):

1. **Информация**
2. **Носитель информации**
3. Система обработки информации
4. Информационная технология
5. **Информационный процесс**

а) 125
б) 234
в) 245
г) 134

56. Укажите все мероприятия, направленные на обеспечение конфиденциальности информации:

1. **Установка паролей для доступа к электронным документам**
2. Создание резервных копий важных файлов
3. Контроль изменений, вносимых в важную информацию легальными пользователями
4. Контроль надежности работы оборудования информационной системы

5. **Установка запрета на запись служебных документов на съемные носители информации**
6. Уничтожение носителей важной информации при помощи специального оборудования

а) 23
б) 45
в) 16
г) 15

57. Укажите все мероприятия, направленные на обеспечение целостности информации:
1. **Ведение журнала регистрации изменений, внесенных в базу данных зарегистрированными пользователями**
2. **Использование надежных носителей информации, замена при истечении гарантийного срока**
3. **Проведение профилактических работ с оборудованием информационной системы**
4. Ограничение прав пользователей на запись в важные файлы
5. Запрет отправки определенных документов по электронной почте

а) 123
б) 345
в) 145
г) 235

58. Информация в зависимости от категории доступа к ней подразделяется на:
1. **общедоступную**
2. широкого доступа
3. **ограниченного доступа**
4. конфиденциальную

а) 23
б) 13
в) 14
г) 24

59. ФСТЭК:
Выберите один ответ:
а) Федеральная служба технологического и экспертного контроля
б) Федеральная служба технического и эксплуатационного контроля
в) Федеральная служба по техническому и экспортному контролю
г) Федеральная служба по техническому и экспертному контролю

60. "**Несанкционированный доступ**" (НСД) к информации - это:
а) доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств
б) доступ, реализующий возможности совокупности физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация

в) доступ с использованием совокупности средств технической разведки и прочих средств, которыми добывается защищаемая информация
г) доступ к информации, реализуемый путём уничтожения технических средств информационной системы

61. **Специальные категории персональных данных** - это:
1. **состояние интимной жизни**
2. **политические взгляды**
3. **национальная принадлежность**
4. сверхъестественные способности
5. состояние аппетита
6. территориальное размещение

а) 123
б) 345
в) 156
г) 235

62. Лицензирование деятельности по распространению шифровальных (криптографических) средств, осуществляет:
Выберите один ответ:
а) Роскомнадзор
б) ФСБ
в) ФСТЭК
г) Ростехнадзор

63. Лицо, ответственное за организацию обработки ПДн, в частности, обязано:
1. **организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов**
2. осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства РФ о ПДн, за исключением требований к защите ПДн
3. лично вести прием и обработку обращений и запросов субъектов персональных данных или их представителей
4. **осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства РФ о ПДн, в том числе требований к защите персональных данных**
5. **доводить до сведения работников оператора положения законодательства Российской Федерации в области налогообложения юридических лиц**

а) 123
б) 345
в) 145
г) 235

64. Предоставление информации - это:
Выберите один ответ:
а) действия, направленные на получение информации как определённым, так и неопределённым кругом лиц, или передачу информации как определенному, так и неопределённому кругу лиц

б) действия, направленные на распространение сведений в средствах массовой информации
в) действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц
г) действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц

Перечень заданий для оценки уровня сформированности компетенции ОПК-5 (индикатор достижения компетенции ОПК-5.3)

65. Обладатель информации - это:
а) лицо получившее на основании закона или договора право разрешать или ограничивать доступ к информации
б) лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам
в) лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам
г) лицо, самостоятельно создавшее информацию

66. Количеством уровней защищенности персональных данных, определяемых правовыми нормативными документами РФ, является:
Выберите один ответ:
а) 6
б) 4
в) 8
г) 2

67. В российской практике «Регламент услуг Удостоверяющего центра (УЦ)» - это:
а) документ, описывающий внутренний порядок работы сотрудников УЦ
б) документ, определяющий перечень услуг, предоставляемых УЦ на возмездной основе
в) организационный документ, определяющий порядок реализации функций УЦ, осуществления его прав и обязанностей
г) документ, определяющий лицензируемые виды деятельности

68. **Информация ограниченного доступа** – это информация, доступ к которой ограничивается:
а) Федеральными законами
б) Указами Президента Российской Федерации
в) Постановлениями Правительства Российской Федерации
г) Специальными нормативными документами

69. Кто осуществляет межведомственный контроль за обеспечением защиты государственной тайны в органах государственной власти
а) федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности
б) Правительство РФ

в) федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, федеральный орган исполнительной власти, уполномоченный в области обороны, федеральный орган исполнительной власти, уполномоченный в области внешней разведки, федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, и их территориальные органы, на которые эта функция возложена законодательством Российской Федерации

г) федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, федеральный орган исполнительной власти, уполномоченный в области обороны, федеральный орган исполнительной власти, уполномоченный в области внешней разведки, федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации

70. В каком законодательном акте приводится перечень сведений, которые не могут быть отнесены к государственной тайне

а) ФЗ «О сведениях по государственной тайне»
б) Ф Закон РФ «О безопасности» З «О сведениях конфиденциального характера»
в) Закон РФ «О безопасности»
г) Закон РФ «О государственной тайне»

71. Кто осуществляет контроль за обеспечением защиты ГТ:

а) Суды РФ
б) ФСБ России
в) Президент Российской Федерации, Правительство Российской Федерации в пределах полномочий, определяемых Конституцией Российской Федерации, федеральными конституционными законами и федеральными законами
г) Правительство Российской Федерации в пределах полномочий, определяемых Конституцией Российской Федерации, федеральными конституционными законами и федеральными законами

72. Гриф секретности это:

а) реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и(или) в сопроводительной документации на него
б) реквизиты, проставляемые на самом носителе и(или) в сопроводительной документации на него
в) реквизиты, свидетельствующие о степени секретности сведений, проставляемые на самом носителе и(или) в сопроводительной документации на него
г) реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе

73. Количество грифов секретности сведений и их носителей
Выберите один ответ:

а) 4
б) 6
в) 3
г) 5

74. Степени секретности сведений:
1. конфиденциально
2. строго конфиденциально
3. **особой важности**
4. **секретно**
5. коммерческая тайна
6. супер особой важности

а) 24
б) 36
в) 34
г) 15

75. Направления деятельности органов ФСБ
а) разведывательная деятельность пограничная деятельность; обеспечение информационной безопасности
б) контрразведывательная деятельность; борьба с терроризмом; борьба с преступностью; разведывательная деятельность; пограничная деятельность
в) контрразведывательная деятельность; борьба с терроризмом; борьба с преступностью; разведывательная деятельность
г) контрразведывательная деятельность; борьба с терроризмом; борьба с преступностью; разведывательная деятельность; пограничная деятельность; обеспечение информационной безопасности

76. Кем назначается и освобождается от должности директор ФСТЭК
а) Президентом Российской Федерации
б) Председателем Правительства Российской Федерации
в) Президентом РФ по представлению Председателя Правительства РФ
г) Руководителем Минобороны России

77. Кому подведомственен ФСТЭК России
а) Минобороны России
б) Никому
в) ФСБ России
г) СВР России

78. Допуск к государственной тайне это:
а) совокупность информации, информационных технологий, технических средств и персонала, обслуживающего систему
б) совокупность информации, информационных технологий и технических средств
в) процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений
г) процесс получения разрешения для работы с государственной тайной

Перечень заданий для оценки уровня сформированности компетенции ОПК-6 (индикатор достижения компетенции ОПК-6.3)

79. Кто осуществляет межведомственный контроль за обеспечением защиты государственной тайны в органах государственной власти

а) федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, федеральный орган исполнительной власти, уполномоченный в области обороны, федеральный орган исполнительной власти, уполномоченный в области внешней разведки, федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации, и их территориальные органы, на которые эта функция возложена законодательством Российской Федерации

б) федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности

в) Правительство РФ

г) федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности, федеральный орган исполнительной власти, уполномоченный в области обороны, федеральный орган исполнительной власти, уполномоченный в области внешней разведки, федеральный орган исполнительной власти, уполномоченный в области противодействия техническим разведкам и технической защиты информации

80. Основаниями для проведения органами по борьбе с терроризмом мероприятий по борьбе с терроризмом являются:

а) все

б) необходимость пресечения террористического акта

в) необходимость добывания информации о событиях или действиях, создающих угрозу терроризма

г) необходимость выявления лиц, причастных к подготовке и совершению террористического акта

81. Кто возглавляет ФСБ России

а) директор ФСБ России

б) Президент Российской Федерации

в) Председатель Правительства РФ

г) Министр обороны России

82. Доступ к сведениям, составляющим государственную тайну это:

а) санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну

б) санкционированное ознакомление конкретного лица со сведениями, составляющими государственную тайну

в) санкционированное полномочным должностным лицом ознакомление конкретного лица с секретными сведениями

г) ознакомление конкретного лица со сведениями, составляющими государственную тайну

83. Государственная тайна это:

а) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности,

распространение которых может нанести ущерб безопасности Российской Федерации

б) совокупность стратегически значимых сведений

в) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности

г) защищаемые государством сведения в области его военной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации

84. Укажите Общие методы обеспечения ИБ Российской Федерации, приведённые в Доктрине ИБ РФ:

1. **экономические**
2. **организационно-технические**
3. **правовые**
4. финансовые

а) 234

б) 134

в) 123

г) 124

85. Основная функция ФСТЭК

а) обеспечение безопасности информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере

б) выявление возможных каналов утечки информации

в) обеспечение безопасности информации криптографическими средствами защиты в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на безопасность государства в информационной сфере

г) выявление лиц, причастных к подготовке и совершению террористического акта

86. В каком Федеральном законе дано определение термину «Информация»:

а) О техническом регулировании

б) Об информации, информатизации и защите информации

в) Об информации, информационных технологиях и о защите информации

г) О персональных данных

87. Аудит информационной безопасности - это:

а) однократная проверка деятельности организации на соответствие правовых аспектов

б) техническая проверка деятельности организации, проводимая ФСТЭК в рамках регламента проверок

в) систематический, независимый и документируемый процесс получения свидетельств деятельности организации по обеспечению ИБ

г) техническая и документарная проверка деятельности организации

88. Угроза безопасности информации - это:

Выберите один ответ:

а) совокупность условий и факторов, определяющих условия размещения информационной системы в пределах контролируемой зоны

б) совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба

в) совокупность условий и факторов, определяющих степень важности информации

г) совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к улучшению функционирования информационной системы

89. Годом принятия Конституции Российской Федерации является:

а) 1992

б) 1994

в) 1991

г) 1993

90. Раскройте сокращение КСИИ:

а) комплексные системы информационной инфраструктуры

б) критически важные информационные системы и информация

в) ключевые системы информационной инфраструктуры

г) ключевые системы информационных интересов

91. К рекомендуемым методам и способам защиты информации в информационных системах относятся:

а) методы и способы защиты информации от утечки по техническим каналам

б) методы и способы сокрытия информации от внутренних нарушителей

в) методы и способы защиты информации от несанкционированного доступа

г) методы и способы устранения конкурентов

92. «Контролируемая зона» это:

а) пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств

б) часть здания, в котором исключено неконтролируемое пребывание посторонних лиц, транспортных, технических и иных материальных средств

в) помещение, в котором постоянно, независимо от окружающих факторов ведётся систематический контроль и надзор за действиями пользователей

г) пространство (территория, здание, часть здания, помещение), в котором действует особый режим наблюдения за всеми сотрудниками организации

93. Защищаемые помещения - это:

а) помещения, специально предназначенные для проведения конфиденциальных мероприятий

б) помещения, специально предназначенные для размещения технических средств информационной системы

в) помещения, специально предназначенные для хранения носителей конфиденциальной информации

г) помещения, специально предназначенные для хранения носителей конфиденциальной информации и размещения технических средств информационной системы

94. В состав объекта информатизации входят:

1. Сотрудники
2. **Средства обработки информации**
3. **Помещения где установлены технические средства**
4. **Информационные ресурсы**

а) 234
б) 134
в) 123
г) 124

95. По признаку отношений к природе возникновения угрозы классифицируются, как:

1. **Объективные**
2. **Субъективные**
3. Внутренние
4. Внешние

а) 34
б) 13
в) 12
г) 24

96. Возможна ли реализация НСД через элементы информационной инфраструктуры, которые в процессе своего жизненного цикла оказываются за пределами контролируемой зоны?

а) В обычных условиях
б) Да
в) Нет
г) В особых условиях

97. Идентификация и аутентификация субъектов и объектов доступа должна обеспечивать:
Выберите один ответ:

а) проверку целостности объектов доступа
б) проверку содержания инструкции пользователя ИС
в) проверку знания субъектом правил разграничения доступа
г) проверку принадлежности субъекту доступа предъявленного им идентификатора

98. Уязвимость информационной системы - это:

а) совокупность условий и факторов, определяющих потенциально опасные последствия реализации угроз
б) слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации
в) слабость информационной системы, удовлетворяющая требованиям специальных нормативных документов ФСБ
г) слабость информационной системы, удовлетворяющая требованиям специальных нормативных документов ФСТЭК

99. Подключение информационных систем, обрабатывающих служебную тайну к сети Интернет:

а) Допускается только с использованием специально предназначенных для этого средств защиты информации

б) Не допускается

в) Допускается только с использованием средств защиты информации известных производителей

г) Допускается

100. Базовый комплект мер обеспечения безопасности информации включает:

а) устранение технических каналов утечки информации

б) оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему

в) контроль точности, полноты и правильности данных, вводимых в ИС

г) обеспечение целостности ИС и информации

3. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю), описание шкал оценивания

Рейтинг-план дисциплины

7 семестр

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1				
Текущий контроль			**0**	**25**
1. Тестирование	25	1	0	25
Рубежный контроль				**25**
1. Тестирование	25	1	0	25
итого			**0**	**50**
Модуль 2				
Текущий контроль			**0**	**25**
1. Тестирование	25	1	0	25
Рубежный контроль			**0**	**25**
1. Тестирование	25	1	0	25
итого			**0**	**50**
Поощрительные баллы				
1. Выполнение дополнительных заданий (из перечня заданий для практических работ)	2	5	0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
Посещение лекционных занятий			0	-6

Посещение практических занятий	0	-10
Итоговый контроль		
Зачёт	0	0
итого	**0**	**110**

8 семестр

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1				
Текущий контроль			**0**	**25**
1. Тестирование	25	1	0	25
Рубежный контроль				**25**
1. Тестирование	25	1	0	25
итого			**0**	**50**
Модуль 2				
Текущий контроль			**0**	**25**
1. Тестирование	25	1	0	25
Рубежный контроль			**0**	**25**
1. Тестирование	25	1	0	25
итого			**0**	**50**
Поощрительные баллы				
1. Выполнение дополнительных заданий (из перечня заданий для практических работ)	2	5	0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
Посещение лекционных занятий			0	-6
Посещение практических занятий			0	-10
Итоговый контроль				
Зачёт с оценкой			0	0
итого			**0**	**110**

Результаты обучения по дисциплине (модулю) у обучающихся оцениваются по итогам текущего контроля количественной оценкой, выраженной в рейтинговых баллах. Оценке подлежит каждое контрольное мероприятие.

При оценивании сформированности компетенций применяется четырехуровневая шкала «неудовлетворительно», «удовлетворительно», «хорошо», «отлично».

Максимальный балл по каждому виду оценочного средства определяется в рейтинг-плане и выражает полное (100%) освоение компетенции.

Уровень сформированности компетенции «хорошо» устанавливается в случае, когда объем выполненных заданий соответствующего оценочного средства составляет 80-100%; «удовлетворительно» – выполнено 40-80%; «неудовлетворительно» – выполнено 0-40%

Рейтинговый балл за выполнение части или полного объема заданий соответствующего оценочного средства выставляется по формуле:

Рейтинговый балл = k × Максимальный балл,

где k = 0,2 при уровне освоения «неудовлетворительно», k = 0,4 при уровне освоения «удовлетворительно», k = 0,8 при уровне освоения «хорошо» и k = 1 при уровне освоения

«отлично».

Оценка на этапе промежуточной аттестации выставляется согласно Положению о модульно-рейтинговой системе обучения и оценки успеваемости студентов УУНиТ:
На дифференцированном зачете выставляется оценка:
• отлично - при накоплении от 80 до 110 рейтинговых баллов (включая 10 поощрительных баллов),
• хорошо - при накоплении от 60 до 79 рейтинговых баллов,
• удовлетворительно - при накоплении от 45 до 59 рейтинговых баллов,
• неудовлетворительно - при накоплении менее 45 рейтинговых баллов.
На зачете выставляется оценка:
• зачтено - при накоплении от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),
• не зачтено - при накоплении от 0 до 59 рейтинговых баллов.

При получении на экзамене оценок «отлично», «хорошо», «удовлетворительно», на зачёте оценки «зачтено» считается, что результаты обучения по дисциплине (модулю) достигнуты и компетенции на этапе изучения дисциплины (модуля) сформированы.