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 ***Защита персональных данных***

Блок Б1, вариативная часть, Б1.В.ДВ.06.01
цикл дисциплины и его часть (базовая, вариативная, дисциплина по выбору)

Направление

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

Программа

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

Форма обучения

Очная

Для поступивших на обучение в
2020 г.

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

Стерлитамак 2023

1. Перечень компетенций с указанием этапов их формирования и описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Формируемая компетенция (с указанием кода)	Результаты обучения по дисциплине (модулю)	Показатели и критерии оценивания результатов обучения по дисциплине (модулю)				Вид оценочного средства
1	2	3				4
		неуд.	удовл.	хорошо	отлично	
Способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4)	1 этап: Знания	Фрагментарное владение современными навыками разработки внутренних нормативных документов, обеспечивающих защиту персональных данных в информационных системах персональных данных	Неполное владение современными навыками разработки внутренних нормативных документов, обеспечивающих защиту персональных данных в информационных системах персональных данных	В целом сформировавшееся владение современными навыками разработки внутренних нормативных документов, обеспечивающих защиту персональных данных в информационных системах персональных данных	Сформировавшееся систематическое владение современными навыками разработки внутренних нормативных документов, обеспечивающих защиту персональных данных в информационных системах персональных данных	Лабораторные работы №1-№4
	2 этап: Умения	Фрагментарное умение использовать и разрабатывать модели угроз для	Неполное умение использовать и разрабатывать модели угроз для информационных	В целом сформировавшееся умение использовать современные	Сформировавшееся систематическое умение использовать и разрабатывать	Лабораторные работы №5-№10

		информационных систем с учетом их назначения, условий и особенностей функционирования	систем с учетом их назначения, условий и особенностей функционирования	программно-аппаратные средства защиты информации	модели угроз для информационных систем с учетом их назначения, условий и особенностей функционирования	
	3 этап: Владения (навыки / опыт деятельности)	Фрагментарное знание современных подходов к правовой защите информации, к организации контроля над возможными каналами их утечки	Неполное знание современных подходов к правовой защите информации, к организации контроля над возможными каналами их утечки	В целом сформировавшееся знание современных подходов к правовой защите информации, к организации контроля над возможными каналами их утечки	Сформировавшееся систематическое знание современных подходов к правовой защите информации, к организации контроля над возможными каналами их утечки	Тест 1, 2, 3

2. Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Перечень заданий для оценки уровня сформированности компетенции ПК-4 (на этапе «Знания»)

Критерии оценки тестов (в баллах)*:*

- *по 1 баллу выставляется студенту за каждый правильный ответ в задании теста;*
- *0 баллов выставляется студенту, если ответ на тест неправильный.*

Тест 1

1 Что такое политика информационной безопасности
а) Методология защиты информации
б) Идеология информационной безопасности +
в) Концепция защиты информации

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»+

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 этого средств +
г) допускается только с использованием средств защиты известных производителей

6 Специальная проверка это
а) выявление возможных каналов утечки информации Российскими техническими средствами
б) определение соответствия условий эксплуатации ОИ требованиям аттестатов соответствия объектам защиты

в) проверки технических средств на наличие возможно внедренных электронных устройств перехвата информации +

7 Каким документов определяются права человека на доступ к информации?
а) Доктриной ИБ
б) Конституцией +
в) ФЗ «О коммерческой тайне»

8 В соответствии с каким Гостом производится аттестация объекта информатизации?
а) ГОСТ РО 0043-004-2013. +
б) ГОСТ ISO 17799
в) BS 7799

9 Источниками угроз несанкционированного доступа являются:
(выберите все верные варианты ответов)
а) нарушители +
б) природные факторы
в) носители вредоносных программ +
г) аппаратные закладки +
д) отказы оборудования
е) отказы программного обеспечения

10 Основные направления обеспечения информационной безопасности указанные в Доктрине ИБ
а) стратегическое развитие военных конфликтов, которые могут возникнуть в результате применения информационных технологий;
б) совершенствование Вооруженных Сил Российской Федерации
в) прогнозирование, обнаружение и оценка информационных угроз, включая угрозы Вооруженным Силам Российской Федерации в информационной сфере; +
г) содействие обеспечению защиты интересов союзников Российской Федерации в информационной сфере; +

11 Техническими каналами утечки информации, приводящими к возникновению угроз безопасности персональных данных являются:
(выберите все верные варианты ответов)
а) кражи технических средств информационной системы
б) утечки акустической (речевой) информации +
в) утечки информации реализуемые через общедоступные информационные сети
г) утечки видовой информации +
д) утечки информации по каналам побочных электромагнитных излучений +
е) утечки информации реализуемые через интернет

12 Документом, определяющим лицензируемые виды деятельности, является:
а) Постановление правительства РФ от 26 января 2006 г. № 45 Об организации лицензирования отдельных видов деятельности
б) Постановление Правительство РФ от 15 августа 2006 г. № 504 О лицензировании деятельности по технической защите конфиденциальной информации
в) Постановление Правительства РФ от 31 августа 2006 г. № 532 О лицензировании

деятельности по разработке и (или) производству средств защиты конфиденциальной информации
г) ФЗ «О лицензировании отдельных видов деятельности» 99-ФЗ от 4 мая 2011 г. +
д) ФЗ «О техническом регулировании» 184-ФЗ от 27 декабря 2002 г.

13 Средствами защиты информации, подлежащими сертификации являются:
(выберите все верные варианты ответов)
а) строительные материалы, используемые для отделки помещений в которых размещаются отдельные элементы ИСПДн
б) детали интерьера, используемые для размещения ИСПДн
в) средства контроля эффективности применения средств защиты информации +
г) средства контроля эффективности прочности ограждений
д) средства защиты информации (технические, программные, программнотехнические) от НСД, блокировки доступа и нарушения целостности +

14 Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:
а) противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации; +
б) осуществление контроля за населением РФ с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, а также отдельными лицами;
в) повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры; +
г) допущения иностранного контроля за функционированием объектов информатизации, на территории Российской Федерации;

15 Перечислить нормативно-методические документы по анализу угроз и уязвимостей
а) BS 7799-3 +
б) ISO 27005 +
в) BSI IT Baseline Protection Manual +
г) ГОСТ 3328

16 «Информационная система» это:
а) совокупность информации, информационных технологий и технических средств +
б) совокупность информации, информационных технологий, технических средств и персонала, обслуживающего систему
в) совокупность информационных технологий и технических средств
г) совокупность информации, технических средств и персонала, обслуживающего информационную систему

д) совокупность информации, технических средств и персонала, обслуживающего и эксплуатирующего информационную систему

17 Количество категорий внутренних нарушителей для ИСПДн, определяемых нормативными документами ФСТЭК:
а) 4
б) 5
в) 6
г) 7
д) 8 +
е) 9

18 Классами защищённости автоматизированных систем от несанкционированного доступа являются: (выберите все верные варианты ответов)
а 1Е
b 2Г
в 2А+
г 2В
д 3С
е 3Б+

19 Основными элементами ИС являются:
(выберите все верные варианты ответов)
а помещения для размещения технических средств
б персональные данные, содержащиеся в базах данных +
в контролируемая зона
г информационные технологии +
д обслуживающий персонал
е технические средства обработки информации +
ж ограждающие конструкции
з технические средства перевозки материальных носителей информации

20 Каким нормативными документами регламентируется деятельность по выявлению угроз
а) BS 7799 +
б) ISO 27005 +
в) BSI IT Baseline Protection Manual +
г) ГОСТ 3328
д) Приказ ФСТЭК № 31

21 К методам и способам защиты информации в информационных системах относятся методы и способы защиты информации от _____ (Ответ несанкционированного доступа) и методы и способы защиты информации от _____ (Ответ утечки по техническим каналам)

22 Классификация угроз информационной безопасности, по виду активов делиться на угрозы, направленные против _____ (Ответ информационных активов) и угрозы, направленные против _____ (Ответ технических средств)

23 Основные требования к системе защиты автоматизированной системы управления должны содержать - _____ (Ответ класс защищенности) автоматизированной системы управления, перечень _____ (Ответ нормативных правовых актов), локальных правовых актов, _____ (Ответ методических документов), национальных стандартов и стандартов организаций, которым должна _____ (Ответ соответствовать) автоматизированная система управления и объекты защиты автоматизированной системы управления на каждом из ее уровней; +

24 При проектировании системы защиты автоматизированной системы управления необходимо: определять типы _____ (Ответ субъектов доступа (пользователи, процессы и иные субъекты доступа)) и _____ (Ответ объектов доступа), являющихся объектами защиты (автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, программируемые логические контроллеры, исполнительные устройства, иные объекты доступа), определять _____ (Ответ методы управления доступом) (дискреционный, мандатный, ролевой), типы _____ (Ответ доступа) (чтение, запись, выполнение) и правила _____ (Ответ разграничения) доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в автоматизированной системе управления, выбирать меры защиты информации, подлежащие реализации в рамках системы защиты автоматизированной системы управления;

25 Разрабатывать организационно-распорядительные документы по защите информации, определяющие правила и процедуры (политики) включает в себя _____ (Ответ реализацию отдельных мер) защиты информации в автоматизированной системе управления в рамках ее _____ (Ответ системы защиты) и _____ (Ответ планирования мероприятий) по обеспечению защиты информации в автоматизированной системе управления; +

26 Определите класс автоматизированной системы по следующим классификационным признакам: АС, в которой работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности, обрабатывается «Служебная тайна». Класс АС_____

27 Ущерб от реализации риска может быть - _____ и _____ Ответ 7 материальный и нематериальный

28 При внедрении организационных мер защиты информации осуществляются: введение _____ (Ответ ограничений) на действия персонала (пользователей (операторского персонала), администраторов, обеспечивающего персонала), а также на условия эксплуатации, изменение состава и конфигурации _____ и_____ (Ответ технических средств и программного обеспечения), а также _____ (Ответ реализация) правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа.

29 Опишите основные организационно-правовые мероприятия для обеспечения защиты информации в автоматизированной системе

30 Охарактеризуйте операторский уровень многоуровневой системы защиты

31 Опишите процесс внедрения системы защиты автоматизированной системы управления

32 Что такое объект информатизации на промышленном предприятии

33 Дайте развернутую характеристику ISO 27005

ТЕСТ 2

1. К каким мерам защиты относится политика безопасности?

а) к административным;
б) к законодательным;
в) к программно-техническим;
г) к процедурным.

2. В каком из представлений матрицы доступа наиболее просто определить пользователей, имеющих доступ к определенному файлу?

а) CL;
б) списки полномочий субъектов;
в) атрибутные схемы.

3. Как называется свойство информации, означающее отсутствие неправомочных, и не предусмотренных ее владельцем изменений?

а) целостность;
б) апеллируемость;
в) доступность;
г) конфиденциальность;
д) аутентичность.

4. К основным принципам построения системы защиты АИС относятся:

а) открытость;
133
б) взаимозаменяемость подсистем защиты;
в) минимизация привилегий;
г) комплексность;

5. Диспетчер доступа...

а) ... использует базу данных защиты, в которой хранятся правила разграничения 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;

6. Какие предположения включает неформальная модель нарушителя?

а) о возможностях нарушителя;
б) о категориях лиц, к которым может принадлежать нарушитель;
в) о привычках нарушителя;

г) о предыдущих атаках, осуществленных нарушителем;
д) об уровне знаний нарушителя.

7. Что представляет собой доктрина информационной безопасности РФ?

а) нормативно-правовой акт, устанавливающий ответственность за правонарушения в сфере информационной безопасности;
б) федеральный закон, регулирующий правоотношения в области информационной безопасности;
в) целевая программа развития системы информационной безопасности РФ, представляющая собой последовательность стадий и этапов;
г) совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

134

8. К какому виду мер защиты информации относится утвержденная программа работ в области безопасности?

а) политика безопасности верхнего уровня;
б) политика безопасности среднего уровня;
в) политика безопасности нижнего уровня;
г) принцип минимизации привилегий;
д) защита поддерживающей инфраструктуры.

9. Чтобы подписать сообщение электронной цифровой подписью, используются:

а) открытый ключ отправителя;
б) открытый ключ получателя;
в) закрытый ключ отправителя;
г) закрытый ключ получателя.

10. Какова последовательность подписания сообщений с помощью ЭЦП?

а) вычисляется хэш, затем хэш зашифровывается;
б) сообщение зашифровывается, после чего результат хэшируется;
в) при подписании сообщение зашифровывается, при проверке вычисляется хэш;
г) вычисляется хэш исходного сообщения, после чего оно зашифровывается.

11. В чем заключается такое свойство функции хэширования H как стойкость к коллизиям первого рода?

а) Для любого хэша h должно быть практически невозможно вычислить или подобрать такое x, что H(x) = h.

135

б) Должно быть практически невозможно вычислить или подобрать любую пару различных сообщений x и y для которых H(x) = H(y);
в) Длина хэша должна быть фиксированной независимо от длины входного сообщения;

Ключ к тесту: 1а, 2б, 3а, 4б, 5в, 6б, 7б, 8а, 9в, 10в, 11а.

ТЕСТ 3

1. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это....

1. информационная война
2. информационное оружие
3. информационное превосходство

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

1. служебная информация
2. коммерческая тайна
3. банковская тайна
4. конфиденциальная информация

3. Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена

1. конфиденциальность
2. целостность
3. доступность
4. аутентичность
5. апеллируемость

4. Гарантия того, что АС ведет себя в нормальном и внештатном режиме так, как запланировано

1. надежность
2. точность
3. контролируемость
4. устойчивость
5. доступность

5. Способность системы к целенаправленному приспособлению при изменении структуры, технологических схем или условий функционирования, которое спасает владельца АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.

1. принцип системности
2. принцип комплексности
3. принцип непрерывной защиты
4. принцип разумной достаточности
5. принцип гибкости системы

6. В классификацию вирусов по способу заражения входят

1. опасные
2. файловые
3. резидентные
4. загрузочные

5. файлово -загрузочные
6. нерезидентные

7. Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это...
1. комплексное обеспечение И Б
2. безопасность АС
3. угроза И Б
4. атака на АС
5. политика безопасности

8. Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов, называются:
1. компаньон - вирусами
2. черви
3. паразитические
4. студенческие
5. призраки
6. стеле-вирусы

9. К видам системы обнаружения атак относятся :
1. системы, обнаружения атаки на ОС
2. системы, обнаружения атаки на конкретные приложения
3. системы, обнаружения атаки на удаленных БД
4. все варианты верны

10. Автоматизированная система должна обеспечивать
1. надежность
2. доступность
3. целостность
4. контролируемость

11. Основными компонентами парольной системы являются
1. интерфейс администратора
2. хранимая копия пароля
3. база данных учетных записей
4. все варианты верны

12. Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это ....
1. идентификатор пользователя
2. пароль пользователя
3. учетная запись пользователя
4. парольная система

13. К принципам информационной безопасности относятся
1. скрытость
2. масштабность
3. системность
4. законность
5. открытости алгоритмов

14. К вирусам, изменяющим среду обитания относятся:
1. черви
2. студенческие
3. полиморфные
4. спутники

15. Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это...
1. Защита информации
2. Компьютерная безопасность
3. Защищенность информации
4. Безопасность данных

16. Система физической безопасности включает в себя следующие подсистемы:
1. оценка обстановки
2. скрытность
3. строительные препятствия
4. аварийная и пожарная сигнализация

17. Какие степени сложности устройства Вам известны
1. упрощенные
2. простые
3. сложные
4. оптические
5. встроенные

18. К механическим системам защиты относятся:
1. проволока
2. стена
3. сигнализация

19. Какие компоненты входят в комплекс защиты охраняемых объектов:
1. датчики
2. телевизионная система
3. лес

20. К выполняемой функции защиты относится:
1. внешняя защита
2. внутренняя защита

3. все варианты верны

21. Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:
1. Защита информации
2. Компьютерная безопасность
3. Защищенность информации
4. Безопасность данных

22. Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним это:
1. информационная война
2. информационное оружие
3. информационное превосходство

23. Информация позволяющая ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынке товаров, работ или услуг это:
1. государственная тайна
2. коммерческая тайна
3. банковская тайна
4. конфиденциальная информация

24. Гарантия того, что при хранении или передаче информации не было произведено несанкционированных изменений:
1. конфиденциальность
2. целостность
3. доступность
4. аутентичность
5. апеллируемость

25. Гарантия точного и полного выполнения команд в АС:
1. надежность
2. точность
3. контролируемость
4. устойчивость
5. доступность

26. Уровень защиты, при котором затраты, риск, размер возможного ущерба были бы приемлемыми:
1. принцип системности
2. принцип комплексности
3. принцип непрерывности
4. принцип разумной достаточности
5. принцип гибкости системы

27. Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АС от заданного множества угроз безопасности:
1. Комплексное обеспечение информационной безопасности
2. Безопасность АС
3. Угроза информационной безопасности
4. атака на автоматизированную систему
5. политика безопасности

28. Особенностями информационного оружия являются:
1. системность
2. открытость
3. универсальность
4. скрытность

29. К функциям информационной безопасности относятся:
1. выявление источников внутренних и внешних угроз
2. страхование информационных ресурсов
3. защита государственных информационных ресурсов
4. подготовка специалистов по обеспечению информационной безопасности
5. все ответы верны

30. К типам угроз безопасности парольных систем относятся
1. словарная атака
2. тотальный перебор
3. атака на основе психологии
4. разглашение параметров учетной записи
5. все варианты ответа верны

31. К вирусам не изменяющим среду обитания относятся:
1. черви
2. студенческие
3. полиморфные
4. спутники

32. Хранение паролей может осуществляться
1. в виде сверток
2. в открытом виде
3. в закрытом виде
4. в зашифрованном виде
5. все варианты ответа верны

33. Антивирусная программа принцип работы, которой основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых вирусов называется:
1. ревизором
2. иммунизатором
3. сканером

4. доктора и фаги.

34. Указать недостатки, имеющиеся у антивирусной программы ревизор:
1. неспособность поймать вирус в момент его появления в системе
2. небольшая скорость поиска вирусов
3. невозможность определить вирус в новых файлах (в электронной почте, на дискете)
4. все варианты верны

35. В соответствии с особенностями алгоритма вирусы можно разделить на два класса:
1. Вирусы, изменяющие среду обитания, но не распространяющиеся
2. Вирусы, изменяющие среду обитания при распространении
3. Вирусы, не изменяющие среду обитания при распространении
4. Вирусы, не изменяющие среду обитания и не способные к распространению в дальнейшем

36. К достоинствам технических средств защиты относятся:
1. регулярный контроль
2. создание комплексных систем защиты
3. степень сложности устройства
4. Все варианты верны

37. К тщательно контролируемым зонам относятся:
1. рабочее место администратора
2. архив
3. рабочее место пользователя
4. все варианты верны

38. К системам оповещения относятся:
1. инфракрасные датчики
2. электрические датчики
3. электромеханические датчики
4. электрохимические датчики

39. К оборонительным системам защиты относятся:
1. проволочные ограждения
2. звуковые установки
3. дачики
4. покрышки

40. К национальным интересам РФ в информационной сфере относятся:
1.Реализация конституционных прав на доступ к информации
2. Защита информации, обеспечивающей личную безопасность
3. Защита независимости, суверенитета, государственной и территориальной целостности
4. Политическая экономическая и социальная стабильность

5. Сохранение и оздоровлении окружающей среды

Ключ к тесту: 1-1, 2-4, 3-1, 4-1, 5-5, 6-3,6, 7-1, 8-2, 9-4, 10-2,3, 11-1,3, 12-2, 13-3,4,5 14-3,15-1, 16-1,3,4, 17-2,3, 18-1,24, 19-1,2, 20-3,21-2, 22-2, 23-2, 24-2, 25-2,26-4, 27-5, 28-3,4, 29-5, 30-5, 31-1, 32-1,2,4 33-3, 34-4, 35-2,3, 36-2, 37-4, 38-1,2, 39-1,2, 40-1.

Перечень заданий для оценки уровня сформированности компетенции ПК-4 (на этапе «Навыки»)

Критерии оценки (в баллах)*:*

- 4-5 баллов выставляется студенту, если работа выполнена полностью, отчет содержит все необходимые пояснения к выполненному заданию;

- 2-3 балла выставляется студенту, если работа выполнена полностью, однако в отчете содержится неполные пояснения к выполненному заданию;

- 0-1 баллов выставляется студенту, если задание не выполнено или отчет не сдан.

Лабораторная работа №1 «Разработка приказов об организации работ по обеспечению безопасности ПДн»

Литература: Защита персональных данных в информационных системах: лабораторный практикум : практикум : [16+] / авт.-сост. В. И. Петренко, И. В. Мандрица. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2018. – 118 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=494823 (дата обращения: 21.06.2021). – Текст : электронный.

Лабораторная работа №2 «Разработка перечней ПДн, информационных систем ПДн и применяемых средств защиты ПДн »

Литература: Защита персональных данных в информационных системах: лабораторный практикум : практикум : [16+] / авт.-сост. В. И. Петренко, И. В. Мандрица. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2018. – 118 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=494823 (дата обращения: 21.06.2021). – Текст : электронный.

Лабораторная работа №3 «Разработка согласия субъекта ПДн на обработку его ПДн»

Литература: Защита персональных данных в информационных системах: лабораторный практикум : практикум : [16+] / авт.-сост. В. И. Петренко, И. В. Мандрица. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2018. – 118 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=494823 (дата обращения: 21.06.2021). – Текст : электронный.

Лабораторная работа №4 «Разработка уведомительных документов по обработке ПДн»

Литература: Защита персональных данных в информационных системах: лабораторный практикум : практикум : [16+] / авт.-сост. В. И. Петренко, И. В. Мандрица. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2018. – 118 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=494823 (дата обращения: 21.06.2021). – Текст : электронный.

Перечень заданий для оценки уровня сформированности компетенции ПК-4 (на этапе «Умения»)

Лабораторная работа №5 «Разработка частной модели угроз безопасности ПДн при их обработке в ИС»

Литература: Защита персональных данных в информационных системах: лабораторный практикум : практикум : [16+] / авт.-сост. В. И. Петренко, И. В. Мандрица. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2018. – 118 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=494823 (дата обращения: 21.06.2021). – Текст : электронный.

Лабораторная работа №6 «Классификация автоматизированных и информационных системПДн»

Литература: Защита персональных данных в информационных системах: лабораторный практикум : практикум : [16+] / авт.-сост. В. И. Петренко, И. В. Мандрица. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2018. – 118 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=494823 (дата обращения: 21.06.2021). – Текст : электронный.

Лабораторная работа №7 «Разработка плана мероприятий по обеспечению защиты ПДн в ИС ПДн»

Литература: Защита персональных данных в информационных системах: лабораторный практикум : практикум : [16+] / авт.-сост. В. И. Петренко, И. В. Мандрица. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2018. – 118 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=494823 (дата обращения: 21.06.2021). – Текст : электронный.

Лабораторная работа №8 «Разработка требований к системе защиты ПДн»

Литература: Защита персональных данных в информационных системах: лабораторный практикум : практикум : [16+] / авт.-сост. В. И. Петренко, И. В. Мандрица. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2018. – 118 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=494823 (дата обращения: 21.06.2021). – Текст : электронный.

Лабораторная работа №9 «Разработка инструкций по защите ПДн в ИС»

Литература: Защита персональных данных в информационных системах: лабораторный практикум : практикум : [16+] / авт.-сост. В. И. Петренко, И. В. Мандрица. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2018. – 118 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=494823 (дата обращения: 21.06.2021). – Текст : электронный.

Лабораторная работа №10 «Аттестация ИС ПДн по требованиям безопасности информации»

Литература: Защита персональных данных в информационных системах: лабораторный практикум : практикум : [16+] / авт.-сост. В. И. Петренко, И. В. Мандрица. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2018. – 118 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=494823 (дата обращения: 21.06.2021). – Текст : электронный.

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Рейтинг-план дисциплины

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Правовое обеспечение информационной безопасности			0	50
Текущий контроль			0	50
Лабораторная работа №1	5	1	0	5
Лабораторная работа №2	5	1	0	5
Лабораторная работа №3	5	1	0	5
Лабораторная работа №4	5	1	0	5
Лабораторная работа №5	5	1	0	5
Лабораторная работа №6	5	1	0	5
Лабораторная работа №7	5	1	0	5
Лабораторная работа №8	5	1	0	5
Лабораторная работа №9	5	1	0	5
Лабораторная работа №10	5	1	0	5

Рубежный контроль			0	50
Тест 1, 2, 3	1	50	0	50
итого			0	100
Поощрительные баллы				10
1. Активная работа на аудиторных занятиях	-	-	0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение лабораторных занятий			0	-10
Итоговый контроль				
Зачет				
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 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.