Министерство науки и высшего образования РФ

Федеральное государственное автономное образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Хакасский технический институт – филиал федерального государственного
автономного образовательного учреждения высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине Б1.О.17 Информационная безопасность организации

индекс и наименование дисциплины или практики в соответствии с ФГОС ВО и учебным планом

Направление подготовки 09.03.03 Прикладная информатика

код и наименование направления подготовки

Направленность (профиль) 09.03.03.04 Прикладная информатика в государственном и муниципальном управлении

код и наименование направленности

ФГАОУ ВО " СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ"

ФГАОУ ВО "СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ"
E=admin@khti.ru, STREET="УЛ. ЩЕТИНКИНА, Д.27", C=RU, S=19 Республика Хакасия, L=Г. АБАКАН, G=Елена Анатольевна, SN=Бабушкина, T=Директор, OU=ХТИ-ФИЛИАЛ ФГ АОУ ВО СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ, O="ФГАОУ ВО "" СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ""", СНИЛС=06047964876, ОГРН=1022402137460, ИНН ЮЛ=2463011853, ИНН=190101002540, CN="ФГАОУ ВО ""СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ""""
Я подтверждаю этот документ своей удостоверяющей подписью

2023.09.19 13:38:16+07'00'

Абакан 2023

1 Перечень компетенций с указанием индикаторов их достижения, соотнесенных с результатами обучения по дисциплине (модулю), практики и оценочными средствами

Семестр	Код и содержание индикатора компетенции	Результаты обучения	Оценочные средства
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			
5	ОПК-3.1.Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной ибиблиографической культуры спримененим информационно-коммуникационных технологий и сучетом основных требованийинформационной безопасности.	Знать: место информационной безопасности в национальной безопасности страны; концепцию информационной безопасности, конституционные и законодательные основы ее реализации; меры ответственности за деяния, совершенные в сфере информационной деятельности; источники и виды угроз информационной безопасности организации;направления формирования и функционирования комплексной системы защиты информации в организации.	тестовые задания, курсовая работа, вопросы для подготовки к экзамену
5	ОПК-3.2.Умеет решать стандартные задачипрофессиональной деятельности наоснове информационной ибиблиографической культуры спримененим информационно-коммуникационных технологий и сучетом основных требованийинформационной безопасности.	Уметь: выявлять угрозы информационной безопасности организации и строить модель угроз;строить модель нарушителя информационной безопасности организации;строить концептуальную модель защиты информации.	практико-ориентированные задания, курсовая работа, вопросы для подготовки к экзамену
5	ОПК-3.3.Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с	Владеть:навыками формирования требований к информационной системе в рамках информационной безопасности;навыками категорирования объектов критической	практико-ориентированные задания, курсовая работа, вопросы для подготовки к экзамену

	учетом требований информационной безопасности.	информационной инфраструктуры;навыками защиты информации от вредоносных программ и сетевых атак с помощью антивирусных программ, криптографических и других методов защиты.	

2 Типовые оценочные средства или иные материалы, с описанием шкал оценивания и методическими материалами, определяющими процедуру проведения и оценивания достижения результатов обучения

Фонд оценочных средств предназначен для организации контроля и самоконтроля студентов и включает в себя оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине в форме экзамена.

В состав ФОС входят следующие оценочные средства: тестовые задания, практико-ориентированные задания, курсовая работа, вопросы для подготовки к экзамену.

Пример варианта теста. ОПК-3, уровень знать

1. Федеральный закон N 149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации» регулирует отношения, возникающие при:

1) применении информационных технологий (+)
2) обеспечении защиты информации (+)
3) осуществлении права на поиск, получение, передачу, производство и распространение информации (+)
4) осуществлении права на передачу и распространение информации

2. Документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах ...

1) скан-копия бумажного носителя с реквизитами (подписью и/или печатью)
2) электронный документ (+)
3) текстовый файл

3. Установите соответствие свойства информации и его сущности:

Характеристика свойства информации	Свойство
А) Свойство информации, которое заключается в ее существовании в неискаженном виде	1) Конфиденциальность 2) Доступность 3) Целостность
Б) Свойство информации, которое указывает на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации	
В) Свойство, которое характеризует способность системы обеспечивать своевременный доступ субъектов	

к информации	

Ответ: А3Б1В2

4. К конфиденциальной информации относят:
1) служебную тайну (+)
2) персональные данные (+)
3) коммерческую тайну (+)

5. Организация работы с криптографическими (шифровальными) средствами защиты информации и специальными техническими средствами, предназначенными для противодействия утечке по техническим каналам связи находится в компетенции ...

Выберите один ответ:

1) ФСТЭК России
2) Президента России
3) ФСБ России (+)
4) Минобороны России

6. Источниками угроз персональным данным обрабатываемым в ИС обработки персональных данных могут быть:

1) аппаратные закладки (скрытно внедряемые к элементам вычислительной системы устройства) (+)
2) вредоносные программы (троянский конь, черви, вирусы и т. д.) (+)
3) внешние нарушители (+)
4) электротехническое оборудование (обеспечивающее энергией)
5) внутренние нарушители (+)
6) сети радио- и телекоммуникаций

7. Высоким потенциалом обладают нарушители ИБ:

1) спецслужбы государств (+)
2) разработчики ПО
3) хакеры
4) террористические, экстремистские группировки

8. Методы криптографического преобразования информации..

1) Архивирование
2) Кодирование (+)
3) Сжатие (+)
4)Хэширование
5) Стеганография (+)
6) Шифрование (+)

7. Считается, что самая высокая мотивация у следующих видов нарушителей:

1) спецслужбы, разведки иностранных государств
2) террористические и экстремистские группировки (+)

3) лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ

4) лица, целенаправленно действующие, стремящиеся к получению конкурентных преимуществ

5) бывшие работники, которые могут сводить счеты с бывшим работодателем

8.Меры организационной защиты информации: управление рисками, политика безопасности организации, управление персоналом, планирование действий в чрезвычайной ситуации.

Перечисленные меры ОЗИ:

1) морально-этические меры защиты информации
2) законодательные меры защиты информации
3) организационно-технические меры защиты информации
4) административные меры защиты информации (+)

9. Совокупность правил обеспечивающих выполнение требований безопасности на территории и в служебных помещениях режимного объекта и направленных на противодействие внутренним угрозам…

1) пропускной режим
2) внутриобъектовый режим (+)

10.Криптография (от древне-греч. κρυπτος – скрытый и γραφω – пишу) – наука о методах обеспечения....

1) аутентичности и достоверности информации
2) аутентичности и доступности информации
3) аутентичности и целостности информации
4) конфиденциальности и аутентичности информации (+)
5) конфиденциальности и целостности информации
6) конфиденциальности и доступности информации

Пример практико-ориентированного задания. ОПК-3, уровень уметь

Задание:основываясь на описании предметной области организации предыдущей лабораторной работы разработайте модель гипотетического нарушителя информационной безопасностидля данной организации. Модель может быть текстовая, графическая или табличная.

Пример практико-ориентированного задания. ОПК-3, уровень владеть

Задание: примените методику категорирования объекта критической информационной инфраструктуры (КИИ) к выбранному в предыдущем задании объекту.

Примерный перечень тем курсовых работ

1. Базовые элементы деятельности субъектов терроризма и экстремизма в информационном пространстве применительно к организациям использующих религиозный фактор.
2. Свойства информационных поводов применительно к организациям использующих религиозный фактор.
3. Разработка подходов по организации журналирования и анализа событий аудита

в корпоративной инфраструктуре без использования специализированных систем.

4. Система видеоконтроля и управление доступа к обьекту.

5. Антивирус. Анализ антивирусов.

6. Кибервойны и кибертерроризм в сфере высоких технологий.

7. Разработать модель морально-психологического обеспечения информационной безопасности предприятия.

8. Регуляторы в сфере защиты информации.

9. Создание защищённой ЛВС.

10. Система защиты информации в конференцзале.

11. Системы предотвращения утечек конфиденциальной информации DLP.

12. Стандарт шифрования данных DES, реализация его компонентов.

13. Организация инженерно-технической защиты объекта.

14. Индикаторы безопасности экономических систем.

15. Анализ схем мошенничества в сети Интернет.

16. Противодействие конкурентной разведке.

17. Выбор программно-аппаратного средства защиты сервера агентства недвижимости.

18. Формирование модели нарушителя информационной безопасности.

19. Разработка комплекса мероприятий по разграничению прав пользователей в локальной вычислительной сети.

20. Проблемы экономической безопасности в условиях цифровой экономик.

21. Организационные методы контроля эффективности защиты информации на примере вербального объекта информации.

22. Модель угроз и нарушителя.

Перечень вопросов для подготовки к экзамену

Перечень вопросов для подготовки к экзамену

1.Информация как объект защиты. Цели и задачи обеспечения безопасности информации. Субъекты информационных отношений по статусу и по отношению к информации.

2.Концептуальная модель информационной безопасности. Важность и сложность проблемы информационной безопасности.

3.Классификация и общий анализ угроз безопасности информации.

4.Виды информации согласно Доктрине информационной безопасности.

5. Содержание и структура законодательства в области информационной безопасности

6. Обзор основных положений ФЗ «Об информации, информационных технологиях и о защите информации».

7. Обзор основных положений законодательства в области персональных данных.

8.Обзор основных положений законодательства в области интеллектуальной собственности.

9.Обзор основных положений законодательства о коммерческой тайне.

10.Обзор основных положений законодательства о государственной тайне.

11. Обзор основных положений законодательства об электронной подписи.

12.Обзор документов в области юридической ответственности за правонарушения в области информационной безопасности.

13.Классификация угроз безопасности ПСНд.

14.Защита информации от несанкционированного доступа (характеристика основных принципов защиты информации от НСД).

15.Способы предотвращения утечки информации по техническим каналам.

16.Портрет нарушителя информационной безопасности. Криминалистическая характеристика компьютерного преступления.

17. Организационные меры обеспечения защиты информации.

18.Принципы политики безопасности.

19.Роли и обязанности должностных лиц по разработке и внедрению политики безопасности.

20.Концепция системы безопасности предприятия. Основные функции службы безопасности.

21.Категорирование объекта КИИ. Порядок категорирования объектов КИИ.

22.Каналы утечки информации.

23.Средства блокирования каналов утечки информации

24.Методы идентификации и аутентификации пользователей.

25.Идентификационные системы. Методы контроля доступа.

26.Модели защиты информации (модель элементарной защиты, многозвенной, многоуровневой). Виды преград. Определение прочности преград.

27.Физические средства защиты.

28. Аппаратные и программно-технические средства защиты.

29.Организационные способы защиты.

30.Комплексный подход к защите информации.

31.Краткая история криптографии.

32.Основные положения и базовые криптографические понятия.

33.Криптографические протоколы

34.Что такое стеганография? Приведите примеры применения методов стеганографии.

35.Кто такой хакер? Что такое хакерские атаки и каковы методы защиты от них?

36.Что такое частотныйкриптоанализ? Приведите пример дешифрования на его основе.

37. Симметричные алгоритмы шифрования.

38. Асимметричные алгоритмы шифрования.

39. Что такое средства PGP? Какие возможности они предоставляют пользователю?

40.Как оценить стойкость протокола парольной аутентификации? Приведите примеры.

Методические рекомендации, определяющие процедуры оценивания

Критерий оценки тестовых заданий

Тесты формируются в еКурсе дисциплины и позволяют получить результат оценивания автоматически. Тесты состоят из заданий разного типа (множественный выбор, соответствие и др.). Каждый тест оценивается по стобальной шкале. Проходной балл - 70.При не достижении проходного балла рекомендуется повторить теоретический материал и воспользоваться дополнительными попытками прохождения теста до достижения проходного балла.

Критерий оценивания практико-ориентированных заданий

Практико-ориентированные задания оцениваются по шкале «зачтено / не зачтено».

«Зачтено» выставляется обучающемуся, если он выполнил задание.

«Не зачтено» выставляется обучающемуся, если он задание не выполнил.

Критерий оценивания курсовой работы

При оценке курсовой работы учитывается: актуальность работы и практическая значимость; использование современных подходов на исследуемую проблему; качество оформления; четкость изложения доклада на защите; правильность ответов на вопросы; степень самостоятельности выполнения работы; актуальность использованных источников.

Защита курсовой работы включает:

– краткое сообщение автора(ов);

– вопросы к автору(ам) работы и ответы на них;

Защита курсовой работы производится публично (в присутствии студентов, защищающих курсовые работы в этот день).

В соответствии с установленными правилами курсовая работа оценивается по следующей шкале:

Оценка «отлично»: работа выполнена в полном объеме, между разделами установлены переходы, корректно применены методы анализа и моделирования, сделаны выводы, представлена разработка системы; работа оформлена в соответствии с требованиями стандарта университета СТУ 7.5–07–2021; студент продемонстрировал высокий уровень освоения компетенций при ответах на вопросы.

Оценка «хорошо» - работа выполнена в полном объеме, но имеются несущественные недочеты в применении методов и моделирования, проведенном анализе и полученных выводах; работа оформлена в соответствии с требованиями стандарта университета СТУ 7.5–07–2021; студент продемонстрировал достаточно высокий уровень освоения компетенций при ответах на вопросы;

Оценка «удовлетворительно»: работа выполнена в полном объеме, в целом выполнены требования данных методических указаний, но имеются существенные недочеты в применении отдельных методов и моделирования, полученных выводах; имеются отклонения в оформлении от стандарта университета СТУ 7.5–07–2021; студент продемонстрировал низкий уровень освоения компетенций при ответах на вопросы.

Оценка «неудовлетворительно»: работа выполнена с грубыми нарушениями в применении методов и моделирования, в нелогичной последовательности анализа и изложения или не по своему варианту, имеется несоответствие требований стандарта университета СТУ 7.5–07–2021 к оформлению.

По итогам защиты курсовой работы выставляется оценка в ведомость и зачетную книжку студента.

Критерии оценки промежуточной аттестации по дисциплине (экзамен)

Итоговая оценка текущей аттестации по дисциплине определяется как среднее взвешенное балла полученного по стобальной шкале в течение семестра и балла полученного на экзамене. Билет экзамена состоит из двух теоретических вопросов. Структура билета и шкала оценивания представлены в таблице.

Таблица – Шкала оценивания ответа на экзамене

Номер и тип задания билета	Весовой коэффициент	Максимальный балл	Балл
Теоретический вопрос 1	0,5	100	50
Теоретический вопрос 2	0,5	100	50
		ИТОГО	100

Итоговая оценка промежуточной аттестации выставляется в соответствии с бально-рейтинговой системой СФУ как среднее взвешенное балла полученного по стобальной шкале в течение семестра и балла полученного на экзамене и соответствует шкале:

84–100 – отлично,
67–83 – хорошо,
50–66 – удовлетворительно,
менее 50 – неудовлетворительно.

Оценка «**отлично»** (84-100 баллов) выставляется обучающимся, если: дан полный, развернутый ответ на поставленный вопрос; показана совокупность осознанных знаний об объекте изучения, доказательно раскрыты основные положения; ответ четко структурирован, выстроен в логической последовательности; ответ изложен грамотным языком; на все дополнительные вопросы даны четкие, аргументированные ответы; обучающийся показывает систематический характер знаний.

Оценка «**хорошо»** (67-83 баллов) выставляется обучающимся, если: дан полный, развернутый ответ на поставленный вопрос, но были допущены неточности в определении понятий; показано умение выделять существенные и несущественные моменты материала; ответ четко структурирован, выстроен в логической последовательности; ответ изложен научным грамотным языком; на дополнительные вопросы были даны неполные или недостаточно аргументированные ответы; обучающийся показывает систематический характер знаний.

Оценка «**удовлетворительно**» (50-66 баллов) выставляется обучающимся, если: дан неполный ответ на поставленный вопрос; логика и последовательность изложения имеют некоторые нарушения; при изложении теоретического материала допущены ошибки; в ответе не присутствуют доказательные выводы; на дополнительные вопросы даны неточные или не раскрывающие сути проблемы ответы.

Оценка **«неудовлетворительно»** (0-49 балло3) выставляется обучающимся, если: не дан ответ на поставленный вопрос или дан неполный ответ на поставленный вопрос, допущены ошибки в определении понятий; при изложении материала допущены принципиальные ошибки.

Разработчик И.В. Янченко