

МИНОБРНАУКИ РОССИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ НАУКИ
ФЕДЕРАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
«КОЛЬСКИЙ НАУЧНЫЙ ЦЕНТР РОССИЙСКОЙ АКАДЕМИИ НАУК»
(ФИЦ КНЦ РАН)

УТВЕРЖДАЮ

Начальник управления аспирантуры и магистратуры
ФИЦ КНЦ РАН

К.Г.-М.Н., доцент И.В. Чикирёв



подпись

29 июня 2020 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

По дисциплине Б1.В.07 Информационная безопасность организации
указывается цикл (раздел) ОП, к которому относится дисциплина, название дисциплины

для направления подготовки (специальности) 09.04.02 Информационные системы и технологии
код и наименование направления подготовки (специальности)

направленность программы (профиль) Информационные системы предприятий и учреждений
наименование профиля /специализаций/образовательной программы

Квалификация выпускника, уровень подготовки
магистр
(указывается квалификация (степень) выпускника в соответствии с ФГОС ВО)

Апатиты

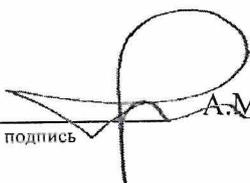
2020

Лист согласования

1. Разработчик:

доцент
должность

УАиМ


подпись А.М. Федоров
И.О. Фамилия

2. Фонд оценочных средств рассмотрен и одобрен на заседании учебно-методической комиссии управления аспирантуры и магистратуры 29 июня 2020 г., протокол № 02.

Председатель УМК УАиМ

29.06.2020

дата

подпись



Л.Д. Кириллова

И.О.Фамилия

Лист переутверждения

Фонд оценочных средств переутвержден на 2021/2022 учебный год без изменений и дополнений.

Председатель УМК УАиМ Л.Д. Кириллова Л.Д. Кириллова

Основание: протокол № 2 от «29» июня 2021 г.

Фонд оценочных средств переутвержден на _____ / _____ учебный год без изменений и дополнений.

Председатель УМК УАиМ _____ Л.Д. Кириллова

Основание: протокол № _____ от « _____ » _____ 20 _____ г

Фонд оценочных средств переутвержден на _____ / _____ учебный год без изменений и дополнений.

Председатель УМК УАиМ _____ Л.Д. Кириллова

Основание: протокол № _____ от « _____ » _____ 20 _____ г

Фонд оценочных средств переутвержден на _____ / _____ учебный год без изменений и дополнений.

Председатель УМК УАиМ _____ Л.Д. Кириллова

Основание: протокол № _____ от « _____ » _____ 20 _____ г

Фонд оценочных средств переутвержден на _____ / _____ учебный год без изменений и дополнений.

Председатель УМК УАиМ _____ Л.Д. Кириллова

Основание: протокол № _____ от « _____ » _____ 20 _____ г

Лист изменений, вносимых в ФОС по дисциплине «Информационная безопасность организации»

В фонд оценочных средств вносятся следующие изменения и дополнения:

1. _____

2. _____

3. _____

Дополнения и изменения внесены и одобрены на заседании учебно-методической комиссии управления аспирантуры и магистратуры ФИЦ КНЦ РАН

от « ____ » _____ г., протокол № _____.

Председатель УМК УАиМ _____ Л.Д. Кириллова

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ
АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

Общие сведения

1.	Отдел	Аспирантуры и магистратуры
2.	Направление подготовки	<u>09.04.02 Информационные системы и технологии</u> Профиль – «<u>Информационные системы предприятий и учреждений</u>»
3.	Дисциплина (модуль)	<u>Б1.В.07 Информационная безопасность организации</u>
4.	Количество этапов формирования компетенций (ДЕ, разделов, тем и т.д.)	7

Перечень компетенций:

- | |
|---|
| <ul style="list-style-type: none">• Способен анализировать и строить оценки и прогнозы в отношении процессов и объектов в профессиональной научной деятельности (ПК-5); |
|---|

Критерии и показатели оценивания компетенций на различных этапах их формирования

Этап формирования компетенции (разделы, темы дисциплины)	Формируемая компетенция	Критерии и показатели оценивания компетенций			Формы контроля сформированности компетенций
		Знать:	Уметь:	Владеть:	
1. Понятие Информационной безопасности. Специфика решений задач информационной безопасности для различных типов предприятий и организаций. Объектно-ориентированный подход для решения задач информационной безопасности.	ПК-5	<ul style="list-style-type: none"> Знать: основные стандарты, средства и методы применения информационных систем и технологий в различных областях профессиональной деятельности (ПК 5.1) 	<ul style="list-style-type: none"> Уметь: с помощью информационных технологий проводить анализ, оценку и прогноз при решении задач в различных областях профессиональной деятельности (ПК 5.2) 	<ul style="list-style-type: none"> Владеть: навыками планирования, организации управления процессами решения задач с помощью подходящих информационных технологий и систем в различных областях профессиональной деятельности (ПК 5.3). 	эссе, раздел перечня вопросов к контрольной работе
2. Классификации угроз информационной безопасности. Корпоративная и персональная "информационная гигиена", "информационные ОБЖ", управление рисками ИБ.	ПК-5	<ul style="list-style-type: none"> Знать: основные стандарты, средства и методы применения информационных систем и технологий в различных областях профессиональной деятельности (ПК 5.1) 	<ul style="list-style-type: none"> Уметь: с помощью информационных технологий проводить анализ, оценку и прогноз при решении задач в различных областях профессиональной 	<ul style="list-style-type: none"> Владеть: навыками планирования, организации управления процессами решения задач с помощью подходящих информационных технологий и систем в различных областях 	эссе, раздел перечня вопросов к контрольной работе

Этап формирования компетенции (разделы, темы дисциплины)	Формируемая компетенция	Критерии и показатели оценивания компетенций			Формы контроля сформированности компетенций
		Знать:	Уметь:	Владеть:	
			деятельности (ПК 5.2)	профессиональной деятельности (ПК 5.3).	
3. Обзор актуальной новостной повестки по теме информационной безопасность на уровнях: государство, крупные корпорации, средний и малый бизнес, профильные сектора экономики и т.п.	ПК-5	<ul style="list-style-type: none"> Знать: основные стандарты, средства и методы применения информационных систем и технологий в различных областях профессиональной деятельности (ПК 5.1) 	<ul style="list-style-type: none"> Уметь: с помощью информационных технологий проводить анализ, оценку и прогноз при решении задач в различных областях профессиональной деятельности (ПК 5.2) 	<ul style="list-style-type: none"> Владеть: навыками планирования, организации и управления процессами решения задач с помощью подходящих информационных технологий и систем в различных областях профессиональной деятельности (ПК 5.3). 	эссе, раздел перечня вопросов к контрольной работе
4. Законодательный уровень информационной безопасности. Доктрина информационной безопасности РФ. Персональные данные. Интеллектуальная собственность, авторские права, служебное произведение, лицензирование.	ПК-5	<ul style="list-style-type: none"> Знать: основные стандарты, средства и методы применения информационных систем и технологий в различных областях профессиональной дея- 	<ul style="list-style-type: none"> Уметь: с помощью информационных технологий проводить анализ, оценку и прогноз при решении задач в различных 	<ul style="list-style-type: none"> Владеть: навыками планирования, организации и управления процессами решения задач с помощью подходящих информационных 	эссе, раздел перечня вопросов к контрольной работе

Этап формирования компетенции (разделы, темы дисциплины)	Формируемая компетенция	Критерии и показатели оценивания компетенций			Формы контроля сформированности компетенций
		Знать:	Уметь:	Владеть:	
		тельности (ПК 5.1)	областях профессиональной деятельности (ПК 5.2)	технологий и систем в различных областях профессиональной деятельности (ПК 5.3).	
5.Административный и процедурный уровни информационной безопасности для предприятий и организаций. Корпоративная политика использования внешних коммуникаций: персональные мобильные устройства, социальные сети, мессенджеры и др. сервисы.	ПК-5	<ul style="list-style-type: none"> Знать: основные стандарты, средства и методы применения информационных систем и технологий в различных областях профессиональной деятельности (ПК 5.1) 	<ul style="list-style-type: none"> Уметь: с помощью информационных технологий проводить анализ, оценку и прогноз при решении задач в различных областях профессиональной деятельности (ПК 5.2) 	<ul style="list-style-type: none"> Владеть: навыками планирования, организации и управления процессами решения задач с помощью подходящих информационных технологий и систем в различных областях профессиональной деятельности (ПК 5.3). 	эссе, раздел перечня вопросов к контрольной работе
6.Классификация программно-технических средств обеспечения информационной безопасности: идентификация и аутентификация; управление доступом, протоколирование, аудит, шифрование,	ПК-5	<ul style="list-style-type: none"> Знать: основные стандарты, средства и методы применения информационных систем и технологий в различных 	<ul style="list-style-type: none"> Уметь: с помощью информационных технологий проводить анализ, оценку и прогноз при 	<ul style="list-style-type: none"> Владеть: навыками планирования, организации и управления процессами решения задач с помощью 	эссе, раздел перечня вопросов к контрольной работе

Этап формирования компетенции (разделы, темы дисциплины)	Формируемая компетенция	Критерии и показатели оценивания компетенций			Формы контроля сформированности компетенций
		Знать:	Уметь:	Владеть:	
электронная цифровая подпись, антивирусная защита		областях профессиональной деятельности (ПК 5.1)	решении задач в различных областях профессиональной деятельности (ПК 5.2)	подходящих информационных технологий и систем в различных областях профессиональной деятельности (ПК 5.3).	
7. Открытые данные информационного пространства и угрозы корпоративной безопасности. Юридические и этические вопросы извлечения и анализа открытых данных социальных сетей. Программные средства анализа социальных сетей. Практические задачи анализа открытых данных социальных сетей.	ПК-5	<ul style="list-style-type: none"> Знать: основные стандарты, средства и методы применения информационных систем и технологий в различных областях профессиональной деятельности (ПК 5.1) 	<ul style="list-style-type: none"> Уметь: с помощью информационных технологий проводить анализ, оценку и прогноз при решении задач в различных областях профессиональной деятельности (ПК 5.2) 	<ul style="list-style-type: none"> Владеть: навыками планирования, организации и управления процессами решения задач с помощью подходящих информационных технологий и систем в различных областях профессиональной деятельности (ПК 5.3). 	эссе, раздел перечня вопросов к контрольной работе
8. Решение задач информационной безопасности при проектировании и разработке информационных систем и программных приложений.	ПК-5	<ul style="list-style-type: none"> Знать: основные стандарты, средства и методы применения информационных 	<ul style="list-style-type: none"> Уметь: с помощью информационных технологий проводить 	<ul style="list-style-type: none"> Владеть: навыками планирования, организации и управления 	эссе, раздел перечня вопросов к контрольной работе

Этап формирования компетенции (разделы, темы дисциплины)	Формируемая компетенция	Критерии и показатели оценивания компетенций			Формы контроля сформированности компетенций
		Знать:	Уметь:	Владеть:	
Использование сторонних сервисов информационной безопасности.		систем и технологий в различных областях профессиональной деятельности (ПК 5.1)	анализ, оценку и прогноз при решении задач в различных областях профессиональной деятельности (ПК 5.2)	процессами решения задач с помощью подходящих информационных технологий и систем в различных областях профессиональной деятельности (ПК 5.3).	

Критерии и шкалы оценивания

1. Тест

Процент правильных ответов	41-60	61-80	81-100
Количество баллов	6	7	8

2. Контрольная работа

Процент правильных ответов	41-60	61-80	81-100
Количество баллов	13	14	15

Оценка	Критерии оценивания ответов контрольной работы
«зачтено»	Обучающийся продемонстрировал знания основных терминов дисциплины, материал изложен последовательно и логично, выводы корректные.
«не зачтено»	Обучающийся не продемонстрировал знания основных терминов дисциплины, материал изложен непоследовательно и нелогично, выводы некорректные.

1. Экзамен

Оценка	Критерии оценивания
«отлично» (20 баллов)	Ставится в том случае, когда обучающийся обнаруживает систематическое и глубокое знание программного материала по дисциплине, умеет свободно ориентироваться в вопросе. Ответ полный и правильный на основании изученного материала. Выдвинутые положения аргументированы и иллюстрированы примерами. Материал изложен в определенной логической последовательности, осознанно, литературным языком, с использованием современных научных терминов; ответ самостоятельный. Обучающийся уверенно отвечает на дополнительные вопросы. Дисциплинарные компетенции сформированы на высоком уровне.
«хорошо» (15 баллов)	Ставится в том случае, когда обучающийся обнаруживает полное знание учебного материала, демонстрирует систематический характер знаний по дисциплине. Ответ полный и правильный, подтвержден примерами; но их обоснование не аргументировано, отсутствует собственная точка зрения. Материал изложен в определенной логической последовательности, при этом допущены 2-3 несущественные погрешности, исправленные по требованию экзаменатора. Обучающийся испытывает незначительные трудности в ответах на дополнительные вопросы. Материал изложен осознанно, самостоятельно, с использованием современных научных терминов, литературным языком. Дисциплинарные компетенции сформированы на продвинутом уровне.
«удовлетворительно» (10 баллов)	Ставится в том случае, когда обучающийся обнаруживает знание основного программного материала по дисциплине, но допускает погрешности в ответе. Ответ недостаточно логически выстроен, самостоятелен. Основные

	<p>понятия употреблены правильно, но обнаруживается недостаточное раскрытие теоретического материала. Выдвигаемые положения недостаточно аргументированы и не подтверждены примерами; ответ носит преимущественно описательный характер. Обучающийся испытывает трудности в ответах на вопросы. Научная терминология используется недостаточно.</p> <p>Дисциплинарные компетенции сформированы на базовом уровне.</p>
<p>«неудовлетворительно» (0 баллов)</p>	<p>Выставляется обучающемуся, обнаружившему пробелы в знаниях основного учебного материала по дисциплине. При ответе обнаружено непонимание обучающимся основного содержания теоретического материала или допущен ряд существенных ошибок, которые обучающийся не может исправить при наводящих вопросах экзаменатора, затрудняется в ответах на вопросы. Ответ носит поверхностный характер; наблюдаются ошибки в использовании научной терминологии.</p> <p>Дисциплинарные компетенции не сформированы.</p>

Пример типового тестового задания

1. Какие основные составляющие информационной безопасности?
 - а) утечка, утрата, кража информации
 - б) доступность, целостность, конфиденциальность информации
 - в) хакеры, майнеры, пранкеры
 - г) вирусы, черви, вредоносное программное обеспечение
2. Какие есть уровни обеспечения информационной безопасности?
 - а) первый, второй, третий, четвёртый
 - б) законодательный, административный, процедурный, программно-технический
 - в) личный, корпоративный, государственный, международный
 - г) общий, для служебного пользования, секретно, совершенно секретно
3. Какие бывают виды угроз информационной безопасности?
 - а) опасные, неопасные
 - б) преднамеренные, случайные
 - в) групповые, одиночные
 - г) объективные, субъективные
4. Какую опасность несет угроза целостности информации?
 - а) информационный источник лишается цели
 - б) информация остается корректной по форме и ложной по содержанию
 - в) информация удаляется целыми блоками
 - г) нарушается заводская упаковка носителя информации
5. Какую опасность несет угроза доступности информации?
 - а) личные сведения становятся общедоступными
 - б) законный потребитель лишается доступа к своей информации
 - в) секретные данные становятся доступны широкому кругу лиц
 - г) открывается доступ к информации, угрожающей жизни и здоровью
6. Какую опасность несет угроза конфиденциальности информации?
 - а) вся открытая информация становится конфиденциальной
 - б) конфиденциальная информация становится доступной посторонним лицам
 - в) конфиденциальная информация удаляется
 - г) доступ к конфиденциальной информации ограничивается

7. Что такое сервис информационной безопасности?
- а) программа, запускаемая на главном сервере в сети
 - б) программная реализация одного из видов защиты информации
 - в) предоставление возможности выбрать уровень защиты информации
 - г) серверный модуль, отвечающий за безопасную коммуникацию
8. Какова функция сервиса аутентификации?
- а) внешний сервис шифрования
 - б) проверка подлинности субъекта информационного взаимодействия
 - в) внутренний сервис учёта доступа к ресурсам
 - г) наделение пользователя уникальным именем
9. Какова функция сервиса протоколирования?
- а) обеспечение работы протокола безопасной передачи данных
 - б) запись в системный журнал происходящих в системе событий
 - в) отметки в протоколе доступа к конфиденциальным данным
 - г) цветовая дифференциация протокольных записей в журнале
10. Какова функция сервиса цифровой подписи?
- а) точно воспроизвести отпечаток подписи отправителя
 - б) подтвердить факт авторства отправителя
 - в) математическими символами заменить обычную подпись
 - г) обеспечить заданную точность при пересылке цифровых данных

Ключ к ответам: 1. б; 2.б; 3. б; 4. б; 5. б; 6. б; 7. б; 8. б; 9. б; 10. б.

Типовые темы контрольной работы

1. Современные правила работы в информационном пространстве - «информационная/цифровая гигиена»
2. Принципы организации безопасной деятельности при работе с современными информационными источниками.
3. Основы безопасности жизнедеятельности (ОБЖ) в современном информационном цифровом мире.
4. Контроль и управление рисками информационной безопасности на работе и дома.
5. Доктрина информационной безопасности Российской Федерации
6. Охрана интеллектуальной собственности
7. Лицензирование результатов интеллектуальной деятельности работников организации. Лицензия GPL.
8. Принципы организации информационной безопасности на предприятии - антикоррупционный подход.
9. Актуальная новостная повестка на различных уровнях.
10. Применение на практике инфраструктуры открытых ключей. PGP-шифрование и цифровая электронная подпись.
11. Социальные сети как угроза корпоративной информационной безопасности.
12. Социальные сети и корпоративная безопасность – риски использования в информационном пространстве организации социальных сетей.
13. Персональные данные как объект защиты информации
14. Персональные данные в европейском законодательстве – GDPR
15. Перспективы использования функций соцсетей на предприятии.
16. Ограничения лицензионного и пользовательского соглашения социальной сети «ВКонтакте»
17. Законодательные и практические аспекты сбора открытых данных из социальных сетей.

**Вопросы к экзамену по дисциплине
«Информационная безопасность организации»**

1. Понятие информационной безопасности. Основные составляющие информационной безопасности.
2. Важность и сложность проблемы информационной безопасности
3. Законодательный уровень информационной безопасности. Российское законодательство в области информационной безопасности
4. Объектно-ориентированный подход к информационной безопасности: основные понятия, достоинства применения
5. Основные определения и критерии классификации угроз
6. Угрозы доступности. Основные угрозы целостности. Угрозы конфиденциальности.
7. Административный уровень информационной безопасности. Политика безопасности информационных систем.
8. Процедурный уровень информационной безопасности: классы мер и принципы их реализации.
9. Программно-технические меры безопасности. Понятие сервиса информационной безопасности. Архитектурная безопасность.
10. Понятие сервиса информационной безопасности. Идентификация и аутентификация. 11. Понятие сервиса информационной безопасности. Управление доступом.
12. Понятие сервиса информационной безопасности. протоколирование и аудит.
13. Понятие сервиса информационной безопасности. управление и анализ защищенности.
14. Понятие сервиса информационной безопасности. обеспечение высокой доступности и отказоустойчивости.
15. Понятие сервиса информационной безопасности. экранирование и туннелирование.
16. Понятие сервиса информационной безопасности. криптография: шифрование.
17. Понятие сервиса информационной безопасности. криптография: контроль целостности.
18. Криптология: базовые понятия и терминология.
19. Криптографические примитивы и их свойства.
20. Модели основных криптоаналитических атак.
21. Антивирусная защита. История развития вирусов и их классификация. Методы защиты от вредоносных программ