10.05.03.07.Б1.О-2021-РП

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»

Институт информационных технологий, машиностроения и автотранспорта

ПОДПИСАНО ЭП КУЗГТУ

Институт информационных технологий,
машиностроения и автотранспорта
Директор

Дата: 01.04.2023 01:04:10

Д.М. Дубинкин

Фонд оценочных средств дисциплины

Основы информационной безопасности

Специальность 10.05.03 Информационная безопасность автоматизированных систем
Специализация / направленность (профиль) Анализ безопасности информационных систем

Присваиваемая квалификация
"Специалист по защите информации"

Формы обучения
очная

5.1 Паспорт фонда оценочных средств

Планируемые результаты обучения по дисциплине (модулю)
Дисциплина направлена на формирование следующих компетенций выпускника:

Форма(ы) текущего контроля	**Компетенции, формируемые в результате освоения дисциплины (модуля)**	**Индикатор(ы) достижения компетенции**	**Результаты обучения по дисциплине (модулю)**	**Уровень**
Опрос по контрольным вопросам или тестирование, подготовка отчетов по практическим и(или) лабораторным работам	ОПК-1 - Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	Владеет основами информационной безопасности, способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе	**Знать** сущность и понятие информационной безопасности, характеристику ее составляющих; основные угрозы безопасности информации; место информационной безопасности в системе национальной безопасности страны. **Уметь** классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности. **Владеть** профессиональной терминологией.	Высокий или средний
Опрос по контрольным вопросам или тестирование, подготовка отчетов по практическим и(или) лабораторным работам	ОПК-12 - Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	Способен применять элементарные знания в области безопасности вычислительных сетей, операционных систем и баз данных	**Знать** источники угроз информационной безопасности и меры по их предотвращению; жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи; современные средства и способы обеспечения информационной безопасности. **Уметь** применять основные правила и документы системы сертификации Российской Федерации; классифицировать основные угрозы безопасности информации. **Владеть** навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем и объектов информатизации; методами защиты информации.	Высокий или средний
Высокий уровень достижения компетенции - компетенция сформирована частично, рекомендованные оценки: отлично, хорошо, зачтено. **Средний уровень достижения компетенции** - компетенция сформирована частично, рекомендованные оценки: хорошо, удовлетворительно, зачтено. **Низкий уровень достижения компетенции** - компетенция не сформирована частично, оценивается неудовлетворительно или не зачтено.				

2. Типовые контрольные задания или иные материалы

Текущий контроль успеваемости и аттестационные испытания обучающихся могут быть организованы с использованием ресурсов ЭИОС КузГТУ. Полный перечень оценочных материалов расположен в ЭИОС КузГТУ.: https://el.kuzstu.ru/login/index.php.

Текущий контроль успеваемости и аттестационные испытания могут проводиться в письменной и (или) устной, и (или) электронной форме.

2.1.Оценочные средства при текущем контроле

Текущий контроль по дисциплине будет заключаться в опросе обучающихся по контрольным вопросам или тестирование по разделу дисциплины, оформлении оформлении отчетов по практическим и(или) лабораторным работам.

Опросе обучающихся по контрольным вопросам или тестирование по разделу дисциплины

Обучающийся отвечает на 2 вопроса, либо отвечает на 10 тестовых заданий.

Критерии оценивания при ответе на вопросы:

- 100 баллов – при правильном и полном ответе на два вопроса;
- 85…99 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 75…84 баллов – при правильном и неполном ответе на два вопроса;
- 65…74 баллов – правильном и полном ответе только на один из вопросов
- 25…64 – при правильном и неполном ответе только на один из вопросов;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–100
Шкала оценивания	Не зачтено	Зачтено

Критерии оценивания при тестировании:

- 100 баллов – при правильном и полном ответе на 10 вопросов;
- 85…99 баллов – при правильном ответе на 8-9 вопросов;
- 75…84 баллов – при правильном ответе на 7 вопросов;
- 65…74 баллов – правильном ответе на 5-6 вопросов
- 25…64 – при правильном ответе только на 4 вопроса;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–64	65–100
Шкала оценивания	Не зачтено	Зачтено

Примерный перечень контрольных вопросов:

1. Информационная безопасность в системе национальной безопасности Российской Федерации.

1. Понятие национальной безопасности. Интересы и угрозы в области национальной безопасности.
2. Влияние процессов информатизации общества на составляющие национальной безопасности и их содержание.
3. Система обеспечения информационной безопасности. Обеспечение информационной безопасности Российской Федерации.
4. Место информационной безопасности в системе национальной безопасности России
5. Государственные структуры, обеспечивающие информационную безопасность государства

2. Основы государственной политики Российской Федерации в области информационной безопасности

1. Основные руководящие документы, регламентирующие вопросы информационной безопасности на уровне государства
2. Основные направления обеспечения безопасности информационных ресурсов государственного значения
3. Как отражены вопросы информационной безопасности государства в конституции РФ и доктрине информационной безопасности РФ о правовом обеспечении информационной сферы?
4. Как отражены вопросы информационной безопасности государства в федеральном законодательстве в сфере информационной безопасности?
5. Международное сотрудничество России в области обеспечения информационной безопасности

3. Информационное противоборство

1. Понятие информационной войны.
2. Проблемы информационной войны. Информационное оружие и его классификация.
3. Цели информационной войны, её составные части и средства её ведения.
4. Информационная война как угроза национальной безопасности.
5. Объекты воздействия в информационной войне.

4. Методы и средства обеспечения информационной безопасности объектов информатизации

1. Классификация методов и средств обеспечения информационной безопасности объектов информатизации
2. Что входит в состав организационно-технических методов обеспечения информационной безопасности?
3. Какие 3 основные аспекта должны учитываться в равной степени, чтобы информация считалась защищенной?
4. От чего зависит набор методов и средств обеспечения информационной безопасности на конкретном объекте информатизации?
5. Назначение и состав системы управления информационной безопасностью

Примерный перечень тестовых заданий:

1. Информационная безопасность в системе национальной безопасности Российской Федерации.

1. В соответствии с военной политикой России направлением обеспечения информационной безопасности в области обороны НЕ является:

Дестабилизация проблемных стран и регионов для последующего их контроля в соответствии с теорией управляемого хаоса
Содействие обеспечению защиты интересов союзников России в информационной сфере
Нейтрализация информационно-психологического воздействия, в т.ч. направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества
Стратегическое сдерживание и предотвращение военных конфликтов, которые могут возникнуть в результате применения информационных технологий

2. Системообразующим фактором национальной безопасности является:

Информационная безопасность
Культурная безопасность
Экономическая безопасность
Религиозная безопасность

3. Информационная безопасность России – это:

Состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов геополитических партнеров и союзников России
Практика защиты ценной информации страны и соответствующих ИС, в целях пресечения посягательств на информацию как со стороны иностранных государств, так и со стороны граждан, не имеющих доступа к ней
Практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации, касающейся деятельности государственных органов России
Состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие России, оборона и безопасность государства

2. Основы государственной политики Российской Федерации в области информационной безопасности

1. Что не относится к объектам информационной безопасности Российской Федерации?

природные и энергетические ресурсы
информационные ресурсы всех видов
информационные системы различного класса и назначения, информационные технологии система формирования общественного сознания

права граждан, юридических лиц и государства на получение, распространение, использование и защиту информации и интеллектуальной собственности

2. Какой законодательный акт регламентирует отношения в области защиты авторских и имущественных прав в области информатизации?

Доктрина информационной безопасности РФ
Закон «О правовой охране программ для ЭВМ и баз данных»
Раздел «Преступления в сфере компьютерной информации» Уголовного кодекса РФ
Указ Президента РФ
Закон «Об информации, информатизации и защите информации»

3. Из нижеперечисленных законодательных актов наибольшей юридической силой в вопросах информационного права обладает

Указ Президента "Об утверждении перечня сведений, относящихся к государственной тайне"
Гражданский кодекс РФ
Закон "Об информации, информатизации и защите информации"
Конституция

3. Информационное противоборство

1. Поражающее воздействие информационного оружия прежде всего направлено на …

Варианты ответа:

мозг человека
информационные системы
информационные продукты
трансграничные информационно — телекоммуникационные сети

2. Не являются методами информационной войны …

Варианты ответа:

подавление элементов инфраструктуры государственного управления
террористические провокации
радиоэлектронная разведка
электронно-магнитное воздействие
деятельность хакеров

3. Информационная война – это …

Варианты ответа:

действия военных структур, направленные на достижение информационного превосходства при одновременном обеспечении собственной безопасности и защиты
любые действия, направленные на поддержку национальной военной стратегии путем воздействия на информацию и информационные системы противника при одновременном обеспечении собственной безопасности и защиты
противоправные действия, направленные на достижение информационного превосходства путем активного воздействия на информацию и информационные системы противника с помощью недостоверной или неполной информации при одновременном обеспечении собственной безопасности и защиты
уничтожение или повреждение информационных систем противника
любые действия, направленные на достижение информационного превосходства, на поддержку национальной военной стратегии путем активного воздействия на информацию и информационные системы противника для достижения поставленных целей при одновременном обеспечении собственной безопасности и защиты

4. Методы и средства обеспечения информационной безопасности объектов информатизации

1. **К основным принципам обеспечения информационной безопасности относится:**

Экономической эффективности системы безопасности
Многоплатформенной реализации системы
Усиления защищенности всех звеньев системы

2. **Окончательно, ответственность за защищенность данных в компьютерной сети несет:**

Владелец сети
Администратор сети
Пользователь сети

3. **Наиболее важным при реализации защитных мер политики безопасности является:**

Аудит, анализ затрат на проведение защитных мер
Аудит, анализ безопасности
Аудит, анализ уязвимостей, риск-ситуаций

Отчеты по лабораторным и (или) практическим работам (далее вместе - работы):

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате (согласно перечню лабораторных и(или) практических работ п.4 рабочей программы).

Содержание отчета:

1.Тема работы.

2. Задачи работы.

3. Краткое описание хода выполнения работы.

4. Ответы на задания или полученные результаты по окончании выполнения работы (в зависимости от задач, поставленных в п. 2).

5. Выводы

Критерии оценивания:

- 75 – 100 баллов – при раскрытии всех разделов в полном объеме
- 0 – 74 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0–74	75–100
Шкала оценивания	Не зачтено	Зачтено

5.2.2 Оценочные средства при промежуточной аттестации

Формами промежуточной аттестации являютя экзамен, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:

ответы на вопросы во время опроса по разделам дисциплины или пройденное тестирование.
зачтенные отчеты обучающихся по лабораторным и(или) практическим работам;

На экзамене обучающийся отвечает на 2 вопроса, либо отвечает на 20 тестовых заданий

Критерии оценивания при ответе на вопросы:

- 100 баллов – при правильном и полном ответе на два вопроса;
- 85…99 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 75…84 баллов – при правильном и неполном ответе на два вопроса;
- 65…74 баллов – правильном и полном ответе только на один из вопросов
- 25…64 – при правильном и неполном ответе только на один из вопросов;
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–24	25-64	65-74	85-99	100
Шкала оценивания	Неуд		Хорошо	Отлично	
	не зачтено		зачтено		

Критерии оценивания при тестировании:

- 95-100 баллов – при правильном и полном ответе на 19-20 вопросов;
- 85…94 баллов – при правильном ответе на 16-18 вопросов;
- 75…84 баллов – при правильном ответе на 13-15 вопросов;
- 65…74 баллов – правильном ответе на 10-12 вопросов
- 25…64 – при правильном ответе только на 1-9 вопрос(ов);
- 0…24 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0–24	25-64	65-74	85-94	95-100
Шкала оценивания	Неуд		Хорошо	Хорошо	Отлично
	не зачтено		зачтено		

Примерный перечень вопросов на экзамен:

1. Понятие национальной безопасности.

2. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
3. Определение информационной безопасности
4. Место информационной безопасности в системе национальной безопасности
5. Интересы личности в информационной сфере
6. Интересы общества в информационной сфере
7. Интересы государства в информационной сфере
8. Угрозы информационному обеспечению государственной политики Российской Федерации
9. Виды угроз информационной безопасности
10. Внешние источники угроз информационной безопасности
11. Внутренние источники угроз информационной безопасности государства.
12. Информационное оружие, его классификация и возможности.
13. Доктрина информационной войны
14. Методы и средства ведения информационной войны
15. Понятие информационного противоборства
16. Причины искажения информации,
17. Виды искажения информации
18. Каналы утечки информации
19. Естественные и искусственные каналы утечки информации
20. Правовые, организационно-технические и экономические методы обеспечения информационной безопасности.
21. Критерии и классы защищенности средств ВТ
22. Компьютерная система как объект информационной безопасности.
23. Информационные процессы как объект информационной безопасности
24. Влияние человеческого фактора на обеспечение информационной безопасности
25. Программно-аппаратные средства обеспечения информационной безопасности.
26. Классификация программно-аппаратных средств обеспечения информационной безопасности
27. Защита от несанкционированного доступа
28. Антивирусная защита
29. Межсетевые экраны
30. VPN-технологии
31. Криптографические методы защиты информации

Примерный перечень тестовых заданий на экзамен:

1. В соответствии с военной политикой России направлением обеспечения информационной безопасности в области обороны НЕ является:

Дестабилизация проблемных стран и регионов для последующего их контроля в соответствии с теорией управляемого хаоса
Содействие обеспечению защиты интересов союзников России в информационной сфере
Нейтрализация информационно-психологического воздействия, в т.ч. направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества
Стратегическое сдерживание и предотвращение военных конфликтов, которые могут возникнуть в результате применения информационных технологий

1. Системообразующим фактором национальной безопасности является:

Информационная безопасность
Культурная безопасность
Экономическая безопасность
Религиозная безопасность

1. Информационная безопасность России – это:

Состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов геополитических партнеров и союзников России
Практика защиты ценной информации страны и соответствующих ИС, в целях пресечения посягательств на информацию как со стороны иностранных государств, так и со стороны граждан, не имеющих доступа к ней
Практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации, касающейся деятельности государственных органов России
Состояние защищенности личности, общества и государства от внутренних и внешних

информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие России, оборона и безопасность государства

1. Что не относится к объектам информационной безопасности Российской Федерации?

природные и энергетические ресурсы
информационные ресурсы всех видов
информационные системы различного класса и назначения, информационные технологии система формирования общественного сознания
права граждан, юридических лиц и государства на получение, распространение, использование и защиту информации и интеллектуальной собственности

1. Какой законодательный акт регламентирует отношения в области защиты авторских и имущественных прав в области информатизации?

Доктрина информационной безопасности РФ
Закон «О правовой охране программ для ЭВМ и баз данных»
Раздел «Преступления в сфере компьютерной информации» Уголовного кодекса РФ
Указ Президента РФ
Закон «Об информации, информатизации и защите информации»

1. Из нижеперечисленных законодательных актов наибольшей юридической силой в вопросах информационного права обладает

Указ Президента "Об утверждении перечня сведений, относящихся к государственной тайне"
Гражданский кодекс РФ
Закон "Об информации, информатизации и защите информации"
Конституция

1. Поражающее воздействие информационного оружия прежде всего направлено на …

мозг человека
информационные системы
информационные продукты
трансграничные информационно — телекоммуникационные сети

1. Не являются методами информационной войны …

подавление элементов инфраструктуры государственного управления
террористические провокации
радиоэлектронная разведка
электронно-магнитное воздействие
деятельность хакеров

1. Информационная война – это …

действия военных структур, направленные на достижение информационного превосходства при одновременном обеспечении собственной безопасности и защиты
любые действия, направленные на поддержку национальной военной стратегии путем воздействия на информацию и информационные системы противника при одновременном обеспечении собственной безопасности и защиты
противоправные действия, направленные на достижение информационного превосходства путем активного воздействия на информацию и информационные системы противника с помощью недостоверной или неполной информации при одновременном обеспечении собственной безопасности и защиты
уничтожение или повреждение информационных систем противника
любые действия, направленные на достижение информационного превосходства, на поддержку национальной военной стратегии путем активного воздействия на информацию и информационные системы противника для достижения поставленных целей при одновременном обеспечении собственной безопасности и защиты

1. К основным принципам обеспечения информационной безопасности относится:

Экономической эффективности системы безопасности

Многоплатформенной реализации системы
Усиления защищенности всех звеньев системы

1. Окончательно, ответственность за защищенность данных в компьютерной сети несет:

Владелец сети
Администратор сети
Пользователь сети

1. Наиболее важным при реализации защитных мер политики безопасности является:

Аудит, анализ затрат на проведение защитных мер
Аудит, анализ безопасности
Аудит, анализ уязвимостей, риск-ситуаций

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

1. Текущий контроль успеваемости обучающихся, осуществляется в следующем порядке: в конце завершения освоения соответствующей темы обучающиеся, по распоряжению педагогического работника, убирают все личные вещи, электронные средства связи и печатные источники информации.

Для подготовки ответов на вопросы обучающиеся используют чистый лист бумаги любого размера и ручку. На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения текущего контроля успеваемости.

Научно-педагогический работник устно задает два вопроса, которые обучающийся может записать на подготовленный для ответа лист бумаги.

В течение установленного научно-педагогическим работником времени обучающиеся письменно формулируют ответы на заданные вопросы. По истечении указанного времени листы бумаги с подготовленными ответами обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов текущего контроля успеваемости.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации. В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов текущего контроля соответствует 0 баллов и назначается дата повторного прохождения текущего контроля успеваемости.

Текущий контроль успеваемости обучающихся по результатам выполнения лабораторных и (или) практических работ осуществляется в форме отчета, который предоставляется научно-педагогическому работнику на бумажном и (или) электронном носителе. Научно-педагогический работник, после проведения оценочных процедур, имеет право вернуть обучающемуся отчет для последующей корректировки с указанием перечня несоответствий. Обучающийся обязан устранить все указанные несоответствия и направить отчет научно-педагогическому работнику в срок, не превышающий трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Результаты текущего контроля доводятся до сведения обучающихся в течение трех учебных дней, следующих за днем проведения текущего контроля успеваемости.

Обучающиеся, которые не прошли текущий контроль успеваемости в установленные сроки, обязаны пройти его в срок до начала процедуры промежуточной аттестации по дисциплине в соответствии с расписанием промежуточной аттестации.

Результаты прохождения процедур текущего контроля успеваемости обучающихся учитываются при оценивании результатов промежуточной аттестации обучающихся.

1. Промежуточная аттестация обучающихся проводится после завершения обучения по дисциплине в семестре в соответствии с календарным учебным графиком и расписанием промежуточной аттестации.

Для успешного прохождения процедуры промежуточной аттестации по дисциплине обучающиеся должны:

1. получить положительные результаты по всем предусмотренным рабочей программой формам текущего контроля успеваемости;
2. получить положительные результаты аттестационного испытания.

Для успешного прохождения аттестационного испытания обучающийся в течение времени,

установленного научно-педагогическим работником, осуществляет подготовку ответов на два вопроса, выбранных в случайном порядке.

Для подготовки ответов используется чистый лист бумаги и ручка.

На листе бумаги обучающиеся указывают свои фамилию, имя, отчество (при наличии), номер учебной группы и дату проведения аттестационного испытания.

При подготовке ответов на вопросы обучающимся запрещается использование любых электронных и печатных источников информации.

По истечении указанного времени, листы с подготовленными ответам на вопросы обучающиеся передают научно-педагогическому работнику для последующего оценивания результатов промежуточной аттестации.

В случае обнаружения научно-педагогическим работником факта использования обучающимся при подготовке ответов на вопросы указанные источники информации – оценка результатов промежуточной аттестации соответствует 0 баллов и назначается дата повторного прохождения аттестационного испытания.

Результаты промежуточной аттестации обучающихся размещаются в ЭИОС КузГТУ.

Текущий контроль успеваемости и промежуточная аттестация обучающихся могут быть организованы с использованием ЭИОС КузГТУ, порядок и формы проведения текущего контроля успеваемости и промежуточной аттестации обучающихся при этом не меняется.