**Министерство науки и высшего образования РФ**
**Федеральное государственное бюджетное образовательное учреждение высшего образования**
**«Национальный исследовательский университет «МЭИ»**

**Направление подготовки/специальность: 10.03.01 Информационная безопасность**

**Наименование образовательной программы: Безопасность автоматизированных систем**

**Уровень образования: высшее образование - бакалавриат**

**Форма обучения: Очная**

# Оценочные материалы
# по дисциплине
# Основы информационной безопасности

**Москва**
**2022**

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:**

| | | |
|---|---|---|
| Преподаватель | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»<br>Сведения о владельце ЦЭП МЭИ<br>Владелец: Потехецкий С.В.<br>Идентификатор: R83b30a44-PotekhetskySV-31b213( | С.В. Потехецкий |
| (должность) | (подпись) | (расшифровка подписи) |

**СОГЛАСОВАНО:**

| | | |
|---|---|---|
| Руководитель образовательной программы | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»<br>Сведения о владельце ЦЭП МЭИ<br>Владелец: Баронов О.Р.<br>Идентификатор: R90d76356-BaronovOR-7bf8fd7e | О.Р. Баронов |
| (должность, ученая степень, ученое звание) | (подпись) | (расшифровка подписи) |
| Заведующий выпускающей кафедры | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»<br>Сведения о владельце ЦЭП МЭИ<br>Владелец: Невский А.Ю.<br>Идентификатор: R4bc65573-NevskyAY-0b6e493d | А.Ю. Невский |
| (должность, ученая степень, ученое звание) | (подпись) | (расшифровка подписи) |

## ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки: достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. ОПК-1 способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства

ИД-2 Понимает значение информационной безопасности для обеспечения объективных потребностей личности, общества и государства

2. ОПК-5 способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности

ИД-1 Использует основы правовых знаний в различных сферах деятельности

3. ОПК-10 способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты

ИД-1 Участвует в работах по реализации политики информационной безопасности, применяет комплексный подход к обеспечению информационной безопасности объекта защиты

и включает:

**для текущего контроля успеваемости:**

Форма реализации: Билеты (письменный опрос)

1. Тест № 3; Тест № 4 (Тестирование)
2. Тест №5 (Тестирование)
3. Тест №6 (Тестирование)

Форма реализации: Проверка задания

1. Тест № 1; Тест № 2 (Тестирование)

**БРС дисциплины**

1 семестр

| Раздел дисциплины | Веса контрольных мероприятий, % | | | | |
|---|---|---|---|---|---|
| | Индекс КМ: | КМ-1 | КМ-2 | КМ-3 | КМ-4 |
| | Срок КМ: | 4 | 8 | 12 | 15 |
| Основные составляющие информационной безопасности | | | | | |
| 1. Вводная лекция | | + | + | | |

| | | | | |
|---|---|---|---|---|
| Тема 2. Основные положения системного подхода к обеспечению информационной безопасности. | | | | + |
| Базовые основы защиты информации | | | | |
| Организационно-правовое и кадровое обеспечение системы информационной безопасности | + | + | + | + |
| Финансово-экономическое обеспечение системы информационной безопасности | | | | + |
| Инженерно-техническое обеспечение системы информационной безопасности. Силы и средства | + | + | + | + |
| Программно-аппаратное обеспечение системы информационной безопасности. Силы и средства | + | + | | + |
| Аудит системы информационной безопасности | | + | | + |
| Вес КМ: | 20 | 25 | 25 | 30 |

$Общая часть/Для промежуточной аттестации$

**СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ**

***I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций***

| Индекс компетенции | Индикатор | Запланированные результаты обучения по дисциплине | Контрольная точка |
|---|---|---|---|
| ОПК-1 | ИД-2$_{ОПК-1}$ Понимает значение информационной безопасности для обеспечения объективных потребностей личности, общества и государства | Знать:<br>организационные меры по защите информации<br>основные угрозы безопасности информации и модели нарушителя в автоматизированных системах<br>основные угрозы безопасности информации и модели нарушителя в автоматизированных системах<br>методы защиты информации от «утечки» по техническим каналам<br>основные методы управления защитой информации<br>национальные, межгосударственные и международные стандарты в области защиты информации | Тест № 1; Тест № 2 (Тестирование)<br>Тест № 3; Тест № 4 (Тестирование)<br>Тест №5 (Тестирование)<br>Тест №6 (Тестирование) |
| ОПК-5 | ИД-1$_{ОПК-5}$ Использует | Уметь: | Тест № 1; Тест № 2 (Тестирование) |

| | | | |
|---|---|---|---|
| | основы правовых знаний в различных сферах деятельности | реализовывать правила разграничения доступа персонала к объектам доступа<br>классифицировать и оценивать угрозы безопасности информации<br>определять подлежащие защите информационные ресурсы автоматизированных систем<br>применять нормативные документы по противодействию технической разведке<br>анализировать программные и программно-аппаратные решения при проектировании системы защиты информации, с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах | Тест № 3; Тест № 4 (Тестирование)<br>Тест №6 (Тестирование) |
| ОПК-10 | ИД-1$_{ОПК-10}$ Участвует в работах по реализации политики информационной безопасности, применяет | Знать:<br>нормативные правовые акты и национальные стандарты по лицензированию в области | Тест № 1; Тест № 2 (Тестирование)<br>Тест № 3; Тест № 4 (Тестирование) |

| | | | |
|---|---|---|---|
| | комплексный подход к обеспечению информационной безопасности объекта защиты | обеспечения защиты государственной тайны и сертификации средств защиты информации руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации нормативные правовые акты в области защиты информации | |

*II. Содержание оценочных средств. Шкала и критерии оценивания*

**КМ-1. Тест № 1; Тест № 2**

**Формы реализации**: Проверка задания
**Тип контрольного мероприятия:** Тестирование
**Вес контрольного мероприятия в БРС:** 20
**Процедура проведения контрольного мероприятия:** Всего вопросов -20 или 40. На вопросы задания даётся по 1 минуте. После проведения тестирования проводится проверка правильности ответов на вопросы и разбор типичных ошибок.

**Краткое содержание задания:**

Тест содержит вопросы **двух уровней сложности**. Вопросы повышенного уровня сложности отмечены звездочкой **(*).**

Тест состоит из **20 или 40** вопросов. При этом как в вопросах, так и в ответах учтена возможность **многовариантности решений.**

Вопросы, предлагающие выбрать **все верные варианты ответа,** имеют от **2** до **4** правильных вариантов ответа. Остальные вопросы имеют единственный правильный вариант ответа.

Ответ на вопрос считается **правильным,** если он является **полным.**

**Во время тестирования запрещается:**

- - пользоваться какой-либо литературой или заранее подготовленными записями;
- - разговаривать с другими тестируемыми;
- - мешать каким-либо способом другим тестируемым;
- - задавать преподавателю вопросы, не относящиеся к процедуре тестирования.

**Контрольные вопросы/задания:**

| | |
|---|---|
| Знать: методы защиты информации от «утечки» по техническим каналам | 1.Человек как основное звено в системе обеспечения ИБ |
| Знать: нормативные правовые акты и национальные стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации | 1.Понятие критических информационных инфраструктур (КИИ) РФ |
| Знать: руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации | 1.Понятие концепции и политики безопасности при обеспечении ЗИ |
| Уметь: определять подлежащие защите информационные ресурсы автоматизированных систем | 1.Модель угроз - это |
| Уметь: реализовывать правила разграничения доступа персонала к объектам доступа | 1.Какой документ ФСТЭК необходимо применять при обосновании актуальных угроз безопасности информации<br>2.Какой международный стандарт описывает |

| | |
|---|---|
| | менеджмент рисков ИБ |

**Описание шкалы оценивания:**

*Оценка:* 5
*Нижний порог выполнения задания в процентах:* 70
*Описание характеристики выполнения знания:* Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

*Оценка:* 4
*Нижний порог выполнения задания в процентах:* 60
*Описание характеристики выполнения знания:* Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

*Оценка:* 3
*Нижний порог выполнения задания в процентах:* 50
*Описание характеристики выполнения знания:* Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

**КМ-2. Тест № 3; Тест № 4**

**Формы реализации**: Билеты (письменный опрос)
**Тип контрольного мероприятия:** Тестирование
**Вес контрольного мероприятия в БРС:** 25
**Процедура проведения контрольного мероприятия:** Всего вопросов -20 или 40. На вопросы задания даётся по 1 минуте. После проведения тестирования проводится проверка правильности ответов на вопросы и разбор типичных ошибок.

**Краткое содержание задания:**
Тест содержит вопросы **двух уровней сложности**. Вопросы повышенного уровня сложности отмечены звездочкой **(*).**
Тест состоит из **20 или 40** вопросов. При этом как в вопросах, так и в ответах учтена возможность **многовариантности решений.**
Вопросы, предлагающие выбрать **все верные варианты ответа,** имеют от **2** до **4** правильных вариантов ответа. Остальные вопросы имеют единственный правильный вариант ответа.
Ответ на вопрос считается **правильным,** если он является **полным.**
**Во время тестирования запрещается:**

- - пользоваться какой-либо литературой или заранее подготовленными записями;
- - разговаривать с другими тестируемыми;
- - мешать каким-либо способом другим тестируемым;
- - задавать преподавателю вопросы, не относящиеся к процедуре тестирования.

**Контрольные вопросы/задания:**

| | |
|---|---|
| Знать: методы защиты информации от «утечки» по техническим каналам | 1.Существуют следующие стратегии обработки риска |
| Знать: нормативные правовые акты в области защиты информации | 1.Модель Шухарта-Деминга состоит из следующих этапов |
| Знать: руководящие и методические документы уполномоченных федеральных органов исполнительной власти | 1.Для поддержания уровня безопасности на должном уровне руководство обязано |

| | |
|---|---|
| по защите информации | |
| Уметь: определять подлежащие защите информационные ресурсы автоматизированных систем | 1.Политика информационной безопасности хозяйствующего субъекта |
| Уметь: применять нормативные документы по противодействию технической разведке | 1.Организации службы ИБ. Подразделение по ЗИ и его основные функции |
| Уметь: реализовывать правила разграничения доступа персонала к объектам доступа | 1.Понятие критических информационных инфраструктур (КИИ) РФ |

**Описание шкалы оценивания:**

*Оценка:* 5
*Нижний порог выполнения задания в процентах:* 70
*Описание характеристики выполнения знания:* Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

*Оценка:* 4
*Нижний порог выполнения задания в процентах:* 60
*Описание характеристики выполнения знания:* Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

*Оценка:* 3
*Нижний порог выполнения задания в процентах:* 50
*Описание характеристики выполнения знания:* Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

**КМ-3. Тест №5**

**Формы реализации**: Билеты (письменный опрос)
**Тип контрольного мероприятия:** Тестирование
**Вес контрольного мероприятия в БРС:** 25
**Процедура проведения контрольного мероприятия:** Всего вопросов -20 или 40. На вопросы задания даётся по 1 минуте. После проведения тестирования проводится проверка правильности ответов на вопросы и разбор типичных ошибок.

**Краткое содержание задания:**
Тест содержит вопросы двух уровней сложности. Вопросы повышенного уровня сложности отмечены звездочкой (*).
Тест состоит из 20 или 40 вопросов. При этом как в вопросах, так и в ответах учтена возможность многовариантности решений.
Вопросы, предлагающие выбрать все верные варианты ответа, имеют от 2 до 4 правильных вариантов ответа. Остальные вопросы имеют единственный правильный вариант ответа.
Ответ на вопрос считается правильным, если он является полным.
Во время тестирования запрещается:

- - пользоваться какой-либо литературой или заранее подготовленными записями;
- - разговаривать с другими тестируемыми;
- - мешать каким-либо способом другим тестируемым;
- - задавать преподавателю вопросы, не относящиеся к процедуре тестирования.

**Контрольные вопросы/задания:**

| | |
|---|---|
| Знать: национальные, межгосударственные и международные стандарты в области защиты информации | 1.Информационная система- это |
| Знать: основные угрозы безопасности информации и модели нарушителя в автоматизированных системах | 1.Предоставление информации - это<br>2.Составляющими угрозы являются |

**Описание шкалы оценивания:**

*Оценка:* 5
*Нижний порог выполнения задания в процентах:* 70
*Описание характеристики выполнения знания:* Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

*Оценка:* 4
*Нижний порог выполнения задания в процентах:* 60
*Описание характеристики выполнения знания:* Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

*Оценка:* 3
*Нижний порог выполнения задания в процентах:* 50
*Описание характеристики выполнения знания:* Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

**КМ-4. Тест №6**

**Формы реализации**: Билеты (письменный опрос)
**Тип контрольного мероприятия:** Тестирование
**Вес контрольного мероприятия в БРС:** 30
**Процедура проведения контрольного мероприятия:** Всего вопросов -20 или 40. На вопросы задания даётся по 1 минуте. После проведения тестирования проводится проверка правильности ответов на вопросы и разбор типичных ошибок.

**Краткое содержание задания:**
Тест содержит вопросы двух уровней сложности. Вопросы повышенного уровня сложности отмечены звездочкой (*).
Тест состоит из 20 или 40 вопросов. При этом как в вопросах, так и в ответах учтена возможность многовариантности решений.
Вопросы, предлагающие выбрать все верные варианты ответа, имеют от 2 до 4 правильных вариантов ответа. Остальные вопросы имеют единственный правильный вариант ответа.
Ответ на вопрос считается правильным, если он является полным.
Во время тестирования запрещается:

- - пользоваться какой-либо литературой или заранее подготовленными записями;
- - разговаривать с другими тестируемыми;
- - мешать каким-либо способом другим тестируемым;
- - задавать преподавателю вопросы, не относящиеся к процедуре тестирования.

**Контрольные вопросы/задания:**

| | |
|---|---|
| Знать: национальные, межгосударственные и международные стандарты в | 1.Дайте определение понятию “информационная безопасность” |

| | |
|---|---|
| области защиты информации | |
| Знать: организационные меры по защите информации | 1.По признаку отношений к природе возникновения угрозы классифицируются как |
| Знать: основные методы управления защитой информации | 1.Сопротивления заземляющих проводников, а также земляных шин должны быть |
| Уметь: анализировать программные и программно-аппаратные решения при проектировании системы защиты информации, с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах | 1.Несанкционированный доступ к информации может быть осуществлён путём |
| Уметь: классифицировать и оценивать угрозы безопасности информации | 1.Требования к защите персональных данных при их обработке в информационных системах персональных данных определяются |
| Уметь: применять нормативные документы по противодействию технической разведке | 1.К угрозам непосредственного доступа в операционную среду компьютера, реализуемым в ходе загрузки операционной системы, относятся |

**Описание шкалы оценивания:**

*Оценка:* 5
*Нижний порог выполнения задания в процентах:* 90
*Описание характеристики выполнения знания:* Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

*Оценка:* 4
*Нижний порог выполнения задания в процентах:* 70
*Описание характеристики выполнения знания:* Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

*Оценка:* 3
*Нижний порог выполнения задания в процентах:* 60
*Описание характеристики выполнения знания:* Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

## СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

**1 семестр**

**Форма промежуточной аттестации:** Экзамен

**Пример билета**

Тестирование по варианту №1
1. Какой номер имеет основной (базовый) закон РФ в области ИБ?
   1. 152
   2. 63
   3. 149
   4. 187
   5. 5

**Процедура проведения**

Экзамен проводится в форме тестирования с ответами на 45 вопросов, из которых на 4 вопроса следует ответить письменно. Время на ответ-60 минут. После проведения проверки правильности ответов на вопросы тестирования, при необходимости задаются 1-2 устных вопроса.

***I. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины***

**1. Компетенция/Индикатор:** ИД-2$_{ОПК-1}$ Понимает значение информационной безопасности для обеспечения объективных потребностей личности, общества и государства

**Вопросы, задания**

1.7. От чего не должны зависеть требования безопасности к информационной системе?
2.8. Какого вида обеспечения СОИБ не предусматривается?
3.10. Дайте определение понятия «Информационная безопасность»
4.12. Какого уровня декомпозиции СОИБ не предполагается?
5.22. Дайте определение целостности
6.23. Главная цель СОИБ ХС - это
7.24. В понятие «государственная тайна» входит информация о…деятельности
8.26. В соответствии с законодательством РФ, информация - это
9.37. Какое направление деятельности не входит в подсистему инженерно-технического обеспечения ИБ?
10.38. В подсистему инженерно – технического обеспечения ХС входят направления
11.39. Управление СОИБ ХС заключается в
12.40. Дайте определение доступности
13.41. Источниками угроз безопасности информации являются
14.42. Термин ОТСС в соответствии с нормативно - методическими документами ФСТЭК означает
15.43. Регулирование деятельности в сфере шифровальных (криптографических) средств осуществляет
16.44. Реализация технического канала утечки информации может привести к нарушению
17.45. Какой номер имеет ФЗ «О персональных данных»?

**Материалы для проверки остаточных знаний**

1.1. Какой номер имеет основной (базовый) закон РФ в области ИБ?

Ответы:

1. 152
2. 63
3. 149
4. 187
5. 5

Верный ответ: 3

2.4. Какого типа антивирусного ПО не существует?

Ответы:

1. Вакцины
2. Ревизоры
3. Детекторы
4. Доктора
5. Фаги
6. Все существуют

Верный ответ: 6

3.5. Какие методы антивирусной защиты относятся к проактивным?

Ответы:

1. Сигнатурные
2. Поведенческий блокиратор
3. Эвристические
4. 1-3
5. 1,3

Верный ответ: 4

**2. Компетенция/Индикатор:** ИД-1$_{ОПК-5}$ Использует основы правовых знаний в различных сферах деятельности

**Вопросы, задания**

1.19. Какой процесс не является основным информационным процессом?

2.20. Какая задача не свойственна для СОИБ организации?

3.21. Какой уровень декомпозиции сложных систем не предусматривается?

**Материалы для проверки остаточных знаний**

1.3. Какими минимальными свойствами должна обладать компьютерная программа, чтобы называться вирусом?

Ответы:

1. Способностью проникать в компьютерные системы
2. Наносить вред компьютеру
3. Создавать свои копии
4. Сообщать о своём присутствии
5. 1,3
6. 1 - 4

Верный ответ: 1,3

**3. Компетенция/Индикатор:** ИД-1$_{ОПК-10}$ Участвует в работах по реализации политики информационной безопасности, применяет комплексный подход к обеспечению информационной безопасности объекта защиты

**Вопросы, задания**

1.1. Какой номер имеет основной (базовый) закон РФ в области ИБ?

2.9. Главная цель СОИБ ХС - это
3.11. Какие требования к СОИБ, обусловленные характером информации, обрабатываемой в ИС, не предъявляются?
4.13. Какое действие не свойственно режиму конфиденциальности информации?
5.14. Какой гриф можно использовать для обозначения коммерческой тайны?
6.15. В формуле вычисления ТСО = Пр + Кр1 + Кр2, Кр - это
7.16. Средства охранного телевидения обеспечивают функционирование этой подсистемы
8.17. Одним из основных условий успешности реализации угроз доступа к ресурсам и сервисам компьютера является
9.18. Какое из перечисленных не является программным средством защиты информации, встроенным в ОС?

**Материалы для проверки остаточных знаний**

1.2. Какой вид тайны информации не является профессиональной?
Ответы:
1. Нотариальная
2. Коммерческая
3. Врачебная
4. Усыновления
5. Исповеди

Верный ответ: 2

***II. Описание шкалы оценивания***

*Оценка:* 5
*Нижний порог выполнения задания в процентах:* 70
*Описание характеристики выполнения знания:* Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений

*Оценка:* 4
*Нижний порог выполнения задания в процентах:* 60
*Описание характеристики выполнения знания:* Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки

*Оценка:* 3
*Нижний порог выполнения задания в процентах:* 50
*Описание характеристики выполнения знания:* Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. на вопросы углубленного уровня

***III. Правила выставления итоговой оценки по курсу***

Оценка определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ», на основании семестровой и экзаменационной составляющих.