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

**Направление подготовки/специальность: 10.04.01 Информационная безопасность**

**Наименование образовательной программы: Управление информационной безопасностью**

**Уровень образования: высшее образование - магистратура**

**Форма обучения: Очная**

# Оценочные материалы
# по дисциплине
# Управление информационной безопасностью

**Москва**
**2024**

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:**

| | | |
|---|---|---|
| Разработчик | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»<br>Сведения о владельце ЦЭП МЭИ<br>Владелец: Минзов А.С.<br>Идентификатор: R17801759-MinzovAS-e8de8907 | А.С. Минзов |

**СОГЛАСОВАНО:**

| | | |
|---|---|---|
| Руководитель образовательной программы | Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»<br>Сведения о владельце ЦЭП МЭИ<br>Владелец: Минзов А.С.<br>Идентификатор: R17801759-MinzovAS-e8de8907 | А.С. Минзов |
| Заведующий выпускающей кафедрой | 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 |

## 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 обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание

ИД-2 Организовать управление информационной безопасностью

и включает:

**для текущего контроля успеваемости:**

Форма реализации: Выполнение задания

1. Защита курсовой работы (Контрольная работа)

Форма реализации: Защита задания

1. Выполнение и защита контрольного задания № 1 (Домашнее задание)
2. Выполнение и защита контрольного задания № 5 (Деловая игра)

Форма реализации: Компьютерное задание

1. Выполнение и защита контрольного задания № 2 (Отчет)
2. Выполнение и защита контрольного задания № 3 (Домашнее задание)
3. Выполнение и защита контрольного задания № 4 (Домашнее задание)
4. Тест №1 (Тестирование)
5. Тест №2 (Тестирование)

**БРС дисциплины**

2 семестр

| Раздел дисциплины | Веса контрольных мероприятий, % | | | | |
|---|---|---|---|---|---|
| | Индекс КМ: | КМ-1 | КМ-2 | КМ-3 | КМ-4 |
| | Срок КМ: | 4 | 8 | 12 | 15 |
| Концепция управления информационной безопасностью | | | | | |
| Введение в дисциплину. | | + | + | + | + |
| Разработка плана и концепции СМИБ. | | + | + | + | + |
| Политика информационной безопасности и технология её разработки. | | + | + | + | + |
| | Вес КМ: | 25 | 25 | 25 | 25 |

3 семестр

| Раздел дисциплины | Веса контрольных мероприятий, % | | | | |
|---|---|---|---|---|---|
| | Индекс КМ: | КМ-1 | КМ-2 | КМ-3 | КМ-4 |

| | Срок КМ: | 4 | 8 | 12 | 15 |
|---|---|---|---|---|---|
| Управление рисками информационной безопасности | | | | | |
| Понятие риск информационной безопасности | | + | + | + | + |
| | Вес КМ: | 25 | 25 | 25 | 25 |

**БРС курсовой работы/проекта**

3 семестр

| Раздел дисциплины | Веса контрольных мероприятий, % | | | |
|---|---|---|---|---|
| | Индекс КМ: | КМ-1 | КМ-2 | КМ-3 |
| | Срок КМ: | 4 | 8 | 13 |
| Введение. КР | | + | | |
| Глава 1. КР | | + | | |
| Глава 2. КР | | | + | |
| Глава 3. КР | | | | + |
| Заключение | | | | + |
| | Вес КМ: | 60 | 20 | 20 |

**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$_{ОПК-1}$ Организовать управление информационной безопасностью | Знать:<br>методы управления СМИБ на основе методик управления рисками<br>основные понятия, термины, определения в сфере управления информационной безопасностью в бизнес-процессах<br>основные нормативные документы по созданию и управлению системой менеджмента информационной безопасности, содержание основных документов необходимых при организации СМИБ<br>Уметь:<br>использовать методы анализа процессов для определения ценности информационных активов организации, | Тест №1 (Тестирование)<br>Выполнение и защита контрольного задания № 1 (Домашнее задание)<br>Выполнение и защита контрольного задания № 2 (Отчет)<br>Выполнение и защита контрольного задания № 3 (Домашнее задание)<br>Тест №2 (Тестирование)<br>Выполнение и защита контрольного задания № 4 (Домашнее задание)<br>Выполнение и защита контрольного задания № 5 (Деловая игра)<br>Защита курсовой работы (Контрольная работа) |

| | | | |
|---|---|---|---|
| | | моделирования актуальных угроз организации<br>применять методы оценки и анализа рисков информационной безопасности организации и создавать документы по управлению СМИБ<br>организовывать работу коллектива и принимать управленческие решения для организации управления информационной безопасностью | |

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

**2 семестр**

**КМ-1. Тест №1**

**Формы реализации**: Компьютерное задание
**Тип контрольного мероприятия:** Тестирование
**Вес контрольного мероприятия в БРС:** 25
**Процедура проведения контрольного мероприятия:** Термины и определения. Требования современных отечественных и международных стандартов по системе менеджмента информационной безопасности (СМИБ). Ответить на вопросы.

**Краткое содержание задания:**
Выбрать верный вариант ответа.

**Контрольные вопросы/задания:**

| | |
|---|---|
| Знать: основные нормативные документы по созданию и управлению системой менеджмента информационной безопасности, содержание основных документов необходимых при организации СМИБ | 1.Резервирование информации включает решение следующих вопросов:<br>a) необходимо определить количество копий, формы их хранения и обновления;<br>b) шифрование копий;<br>c) тестирование копий;<br>d) обеспечение физической защиты;<br>e) централизованное хранение;<br>f) объем (т.е. полное или выборочное резервирование) и частота резервирования должны отражать требования бизнеса организации, требования к безопасности затрагиваемой информации и критичность информации для непрерывной работы организации;<br>g) аудит резервных копий. |
| Знать: основные понятия, термины, определения в сфере управления информационной безопасностью в бизнес-процессах | 1.Управление производительностью информационных систем проводится с целью:<br>a) Прогнозирования производительности оборудования исходя будущих целей обработки информации.<br>b) Оптимизация производительности информационных систем.<br>c) Разработки требований к производительности оборудования по обработки информации. |
| Уметь: использовать методы анализа процессов для определения ценности информационных активов организации, моделирования актуальных угроз организации | 1.Безопасность сетевых услуг включает:<br>a) логически изолированной средой;<br>b) блокированием любого несанкционированного использования мобильной программы;<br>c) не блокированием приема мобильной программы;<br>d) обеспечением уверенности в отсутствии мобильной программы;<br>e) контроле ресурсов доступных мобильной программе; |

| | |
|---|---|
| | f) применением криптографических мер и средств контроля и управления для однозначной аутентификации мобильной программы.<br>2.Вопросы электронной торговли включает:<br>a) Планирование СМИБ электронной торговли.<br>b) Аутентификацию субъектов электронной торговли..<br>c) Авторизацию субъектов электронной торговли.<br>d) Расследование инцидентов.<br>e) Информирование партнеров об условиях их авторизации.<br>f) Создание механизмов неотказуемости сделок.<br>g) Защиту от мошенничества при оплате. |

**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

*Оценка:* 2
*Описание характеристики выполнения знания:* Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

**КМ-2. Выполнение и защита контрольного задания № 1**

**Формы реализации**: Защита задания
**Тип контрольного мероприятия:** Домашнее задание
**Вес контрольного мероприятия в БРС:** 25
**Процедура проведения контрольного мероприятия:** Дать определение термина, и пояснить механизмы его проявления или реализации по варианту, соответствующему номеру в списке группы. Каждому студенту необходимо дать определение по 5 терминам. Результаты оформляются в виде отчета по заданию в формате .doc, включающему титульный лист (наименование университета, института, кафедры), номер и наименование задания, фамилия имя и отчество студента. Отчет включает ответы на 5 вопросов. При анализе уделить внимание тем терминам, которые в разных стандартах сформулированы по разному. На следующем занятии быть готовым изложить содержание своей работы.

**Краткое содержание задания:**
Разработка плана и концепции СМИБ

**Контрольные вопросы/задания:**

| | |
|---|---|
| Знать: основные нормативные документы по созданию и | 1.Непрерывность бизнеса и способы её обеспечения |

| | |
|---|---|
| управлению системой менеджмента информационной безопасности, содержание основных документов необходимых при организации СМИБ | |
| Знать: основные понятия, термины, определения в сфере управления информационной безопасностью в бизнес-процессах | 1.События и их классификация |
| Уметь: использовать методы анализа процессов для определения ценности информационных активов организации, моделирования актуальных угроз организации | 1.Процесс<br>2.Принципы СМИБ |

**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

*Оценка:* 2
*Описание характеристики выполнения знания:* Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

**КМ-3. Выполнение и защита контрольного задания № 2**

**Формы реализации**: Компьютерное задание
**Тип контрольного мероприятия:** Отчет
**Вес контрольного мероприятия в БРС:** 25
**Процедура проведения контрольного мероприятия:** Провести моделирование процессов СМИБ (ГОСТ Р ИСО/МЭК 27001-2006 г., приказов ФСТЭК №17, 21 и пост. Правит. 1119) по одной из предложенных форм: IDEF0, алгоритм или Интеллектуальная карта (ИК). Варианты задания приведены в таблице. Результаты представить в форме отчета в электронной форме в виртуальном университете (http://bc.mpei.ru ). Уровень агрегации процессов выполнить таким образом, чтобы описание модели процессов размещалось с необходимыми комментариями на листе формата А4. Результаты моделирования защищаются студентом на занятии (объясняются процессы, условия их выполнения и результаты). Можно использовать любые технологии для моделирования.

**Краткое содержание задания:**

Разработка формализованных документов СМИБ

**Контрольные вопросы/задания:**

| | |
|---|---|
| Знать: основные нормативные документы по созданию и управлению системой менеджмента информационной безопасности, содержание основных документов необходимых при организации СМИБ | 1.4.2.1 (IDEF0) |
| Знать: основные понятия, термины, определения в сфере управления информационной безопасностью в бизнес-процессах | 1.4.2.1 (алгоритм) |
| Уметь: использовать методы анализа процессов для определения ценности информационных активов организации, моделирования актуальных угроз организации | 1.Пр-з ФСТЭК №17 (алгоритм) |

**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

*Оценка:* 2
*Описание характеристики выполнения знания:* Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

### КМ-4. Выполнение и защита контрольного задания № 3

**Формы реализации**: Компьютерное задание
**Тип контрольного мероприятия:** Домашнее задание
**Вес контрольного мероприятия в БРС:** 25
**Процедура проведения контрольного мероприятия:** На основе стандарта 27002 изучить рекомендованные меры и средства контроля и управления при создании СМИБ. Результаты представить в форме интеллектуальных карт с необходимыми детальными пояснениями (MS visio или Mind Maple Lite). Задания включают разделы ГОСТ 27002.

**Краткое содержание задания:**

Разработка частной политики информационной безопасности. Анализ рекомендованных мер и средств контроля при создании системы СМИБ (ГОСТ 27001, 27002)

**Контрольные вопросы/задания:**

| | |
|---|---|
| Знать: основные нормативные документы по созданию и управлению системой менеджмента информационной безопасности, содержание основных документов необходимых при организации СМИБ | 1.Безопасность, связанная с персоналом |
| Знать: основные понятия, термины, определения в сфере управления информационной безопасностью в бизнес-процессах | 1.Физическая безопасность и защита от воздействий окружающей среды |
| Уметь: использовать методы анализа процессов для определения ценности информационных активов организации, моделирования актуальных угроз организации | 1.Управление доступом |

**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

*Оценка:* 2
*Описание характеристики выполнения знания:* Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

**3 семестр**

**КМ-1. Тест №2**

**Формы реализации**: Компьютерное задание
**Тип контрольного мероприятия:** Тестирование
**Вес контрольного мероприятия в БРС:** 25
**Процедура проведения контрольного мероприятия:** Методы описания рисков

**Краткое содержание задания:**

Выбрать верный вариант ответа.

**Контрольные вопросы/задания:**

| | |
|---|---|
| Знать: методы управления СМИБ на основе методик управления рисками | 1.Роли и обязанности в области безопасности должны включать в себя требования в отношении:<br>a) реализации и действия в соответствии с политиками информационной безопасности организации;<br>b) защиты активов от несанкционированного доступа, разглашения сведений, модификации, разрушений или вмешательства;<br>c) выполнения определенных процессов или деятельности, связанных с безопасностью;<br>d) обеспечения уверенности в том, что на индивидуума возлагается ответственность за предпринимаемые действия;<br>e) создание системы осведомленности сотрудников.<br>f) информирования о событиях или потенциальных событиях, связанных с безопасностью, или других рисках безопасности для организации. |
| Уметь: организовывать работу коллектива и принимать управленческие решения для организации управления информационной безопасностью | 1.В состав активов не включается:<br>a) информация: базы данных и файлы данных, договоры и соглашения, системная документация, исследовательская информация, руководства пользователя, учебные материалы, процедуры эксплуатации или поддержки, планы непрерывности бизнеса, меры по переходу на аварийный режим, контрольные записи и архивированная информация;<br>b) программные активы: прикладные программные средства, системные программные средства, средства разработки и утилиты;<br>c) физические активы: компьютерное оборудование, средства связи, съемные носители информации и другое оборудование;<br>d) услуги: вычислительные услуги и услуги связи, основные поддерживающие услуги, например отопление, освещение, электроэнергия и кондиционирование воздуха;<br>e) корпоративные знания;<br>f) персонал;<br>g) нематериальные ценности, например репутация и имидж организации. |
| Уметь: применять методы оценки и анализа рисков информационной безопасности организации и создавать документы по управлению СМИБ | 1.Круг обязанностей каждого руководителя определяется границами:<br>a) активов и процессов;<br>b) наличием ответственных за каждый актив;<br>c) наличием документов по управлению;<br>d) наличием полномочий и уровней обязанностей. |

**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

*Оценка:* 2
*Описание характеристики выполнения знания:* Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

**КМ-2. Выполнение и защита контрольного задания № 4**

**Формы реализации**: Компьютерное задание
**Тип контрольного мероприятия:** Домашнее задание
**Вес контрольного мероприятия в БРС:** 25
**Процедура проведения контрольного мероприятия:** Провести анализ выявленного аудитором несоответствия (пример в таблице) в системе ин-формационной безопасности (ГОСТ р ИСО/МЭК 27002) и предложить действия по его устранению.

**Краткое содержание задания:**
Разработка плана и концепции СМИБ

**Контрольные вопросы/задания:**

| | |
|---|---|
| Знать: методы управления СМИБ на основе методик управления рисками | 1.Сотрудники организации не сообщают о потенциальных инцидентах информационной безопасности. |
| Уметь: организовывать работу коллектива и принимать управленческие решения для организации управления информационной безопасностью | 1.План осведомленности персонала не отражает реальные требования.<br>2.Результаты мониторинга СМИБ администрацией организации не анализируются, а результаты анализа не фиксируются. |
| Уметь: применять методы оценки и анализа рисков информационной безопасности организации и создавать документы по управлению СМИБ | 1.Политика использования беспроводных систем связи отсутствует. В организации используются общедоступные сети WI-FI. |

**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

*Оценка:* 2
*Описание характеристики выполнения знания:* Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

**КМ-3. Выполнение и защита контрольного задания № 5**

**Формы реализации**: Защита задания
**Тип контрольного мероприятия:** Деловая игра
**Вес контрольного мероприятия в БРС:** 25
**Процедура проведения контрольного мероприятия:** Провести планирование СМИБ организации в соответствие с требованиями стандарта ГОСТ Р ИСО/МЭК 27001-2006 г на основании исходных данных. Организацию планирования СМИБ провести в форме деловой игры с распределением ролей обучающихся в составе группы планирования из 3-4 человек. Исходные данные для планирования находятся в электронном виде в форме задания и методики его выполнения в виртуальном университете.

**Краткое содержание задания:**
Провести планирование СМИБ

**Контрольные вопросы/задания:**

| | |
|---|---|
| Знать: методы управления СМИБ на основе методик управления рисками | 1.Политика информационной безопасности. |
| Уметь: организовывать работу коллектива и принимать управленческие решения для организации управления информационной безопасностью | 1.Результаты комплексного моделирования угроз.<br>2.План обработки рисков. |
| Уметь: применять методы оценки и анализа рисков информационной безопасности организации и создавать документы по управлению СМИБ | 1.Положение о применимости. |

**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

*Оценка:* 2
*Описание характеристики выполнения знания:* Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

**КМ-4. Защита курсовой работы**

**Формы реализации**: Выполнение задания
**Тип контрольного мероприятия:** Контрольная работа
**Вес контрольного мероприятия в БРС:** 25
**Процедура проведения контрольного мероприятия:** Разработка плана по обработке рисков и положения о применимости

**Краткое содержание задания:**
Защита курсовой работы

**Контрольные вопросы/задания:**

| | |
|---|---|
| Знать: методы управления СМИБ на основе методик управления рисками | 1.Разработка алгоритма процессов организации защиты ИСПДН |
| Уметь: организовывать работу коллектива и принимать управленческие решения для организации управления информационной безопасностью | 1.Требования по технической защите информации |
| Уметь: применять методы оценки и анализа рисков информационной безопасности организации и создавать документы по управлению СМИБ | 1.Анализ информационных технологий для поддержки процессов аудита<br>2.Алгоритм процессов организации защиты информации в концепции ГОСТ 27001 |

**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

*Оценка:* 2

*Описание характеристики выполнения знания:* Оценка "неудовлетворительно" выставляется если задание выполнено неверно или преимущественно не выполнено

**Для курсового проекта/работы**

**3 семестр**

***I. Описание КП/КР***

1. Овладеть методами и технологиями создания, внедрения и управления системами информационной безопасности, разработанными в различных концепциях. 2. Показать умения в проведении анализа технологий и методик существующих процессов управления информационной безопасностью организации и выявления путей их дальнейшего развития.

***II. Примеры задания и темы работы***

Пример задания

| №№ | Наименование темы курсовой | Цели (этапы) работы | Рекомендованные источники | Примечание |
|---|---|---|---|---|
| 1 | Методика планирования непрерывности бизнес-процессов (НБП) в СМИБ. | 1. Разработать диаграмму процессов планирования НБП и провести её описание.<br>2. Разработать политику и план НБП на примере организации с учетом модели рисков.<br>3. Определить область применения методики и описать ситуации | ГОСТ Р ИСО/МЭК 27001, 27002 | Можно использовать учебную модель АКБ. |

**Тематика КП/КР:**

Сравнительный анализ практических правил стандарта ГОСТ Р ИСО/МЭК 27002 и требований нормативных документов по защите ГИС.
Методы и технологии защиты ГИС, содержащих биометрические данные больших объемов (свыше 100 000 чел).
Сравнительный анализ практических правил стандарта ГОСТ Р ИСО/МЭК 27002 и требований нормативных документов по защите КИИ.

**КМ-1. Соблюдение графика выполнения КР; качество оформления КР**
**Описание шкалы оценивания**

*Оценка:* 5
*Нижний порог выполнения задания в процентах:* 70
*Описание характеристики выполнения знания:* Оценка 5 («отлично»), если задание получено с опозданием не более чем на 2 недели

*Оценка:* 4
*Нижний порог выполнения задания в процентах:* 60
*Описание характеристики выполнения знания:* Оценка 4 («хорошо»), если задание получено с опозданием не более чем на 3 недели

*Оценка:* 3
*Нижний порог выполнения задания в процентах:* 50
*Описание характеристики выполнения знания:* Оценка 3 («удовлетворительно»), если задание получено с опозданием более чем на 3 недели

*Оценка:* 2
*Описание характеристики выполнения знания:* Оценка 2 («неудовлетворительно»), если задание не выполнено

**КМ-2. Соблюдение графика выполнения КР; оценка выполнения разделов КР**
**Описание шкалы оценивания**

*Оценка:* 5
*Нижний порог выполнения задания в процентах:* 70
*Описание характеристики выполнения знания:* Оценка 5 («отлично»), если задание получено с опозданием не более чем на 2 недели

*Оценка:* 4
*Нижний порог выполнения задания в процентах:* 60
*Описание характеристики выполнения знания:* Оценка 4 («хорошо»), если задание получено с опозданием не более чем на 3 недели

*Оценка:* 3
*Нижний порог выполнения задания в процентах:* 50
*Описание характеристики выполнения знания:* Оценка 3 («удовлетворительно»), если задание получено с опозданием более чем на 3 недели

*Оценка:* 2
*Описание характеристики выполнения знания:* Оценка 2 («неудовлетворительно»), если задание не выполнено

**КМ-3. Соблюдение графика выполнения КР; оценка выполнения разделов КР**
**Описание шкалы оценивания**

*Оценка:* 5
*Нижний порог выполнения задания в процентах:* 70
*Описание характеристики выполнения знания:* Оценка 5 («отлично»), если задание получено с опозданием не более чем на 2 недели

*Оценка:* 4
*Нижний порог выполнения задания в процентах:* 60
*Описание характеристики выполнения знания:* Оценка 4 («хорошо»), если задание получено с опозданием не более чем на 3 недели

*Оценка:* 3
*Нижний порог выполнения задания в процентах:* 50
*Описание характеристики выполнения знания:* Оценка 3 («удовлетворительно»), если задание получено с опозданием более чем на 3 недели

*Оценка:* 2
*Описание характеристики выполнения знания:* Оценка 2 («неудовлетворительно»), если задание не выполнено

## СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

**2 семестр**

**Форма промежуточной аттестации:** Зачет с оценкой

**Процедура проведения**

Зачет проводится в устной форме по билетам согласно программе зачета

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

**1. Компетенция/Индикатор:** ИД-2$_{ОПК-1}$ Организовать управление информационной безопасностью

**Вопросы, задания**

1.Требования современных отечественных и международных стандартов по системе менеджмента информационной безопасности (СМИБ)
2.Концепция управления информационной безопасностью на основе цикла Дёминга-Шухарта
3.Критерии управления информационной безопасностью
4.Разработка плана и концепции СМИБ
5.Логистика процессов управления информационной безопасностью на основе стандартов
6.Система документооборота и её формализованное представление
7.Политика информационной безопасности и технология её разработки
8.Частные политики информационной безопасности
9.Процедуры, регламенты и инструкции по информационной безопасности

**Материалы для проверки остаточных знаний**

1.Управление производительностью информационных систем проводится с целью:
Ответы:
a) Прогнозирования производительности оборудования исходя будущих целей обработки информации.
b) Оптимизация производительности информационных систем.
c) Разработки требований к производительности оборудования по обработки информации.
Верный ответ: a, b
2.Политика ИБ включает:
Ответы:
a) Цели и задачи СМИБ.
b) Концепция СМИБ.
c) Частные политики.
d) Ответственных за организацию СМИБ.
e) Лист изменений.
Верный ответ: a,b,d,e
3.Безопасность при использовании мобильных программ не обеспечивается:
Ответы:
a) логически изолированной средой;
b) блокированием любого несанкционированного использования мобильной программы;
c) не блокированием приема мобильной программы;
d) обеспечением уверенности в отсутствии мобильной программы;

e) контроле ресурсов доступных мобильной программе;
f) применением криптографических мер и средств контроля и управления для однозначной аутентификации мобильной программы.

Верный ответ: a,b,d,e

***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

*Оценка:* 2
*Описание характеристики выполнения знания:* Работа не выполнена или выполнена преимущественно неправильно

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

Оценка определяется по совокупности результатов текущего контроля успеваемости в в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ»

**3 семестр**

**Форма промежуточной аттестации:** Экзамен

**Пример билета**

| | | |
|---|---|---|
| **НИУ МЭИ** | **ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1**<br>Кафедра *Безопасности и информационных технологий*<br>Дисциплина «Управление информационной безопасностью» | *Утверждаю:*<br>*Зав. каф. БИТ*<br>*А.Ю.Невский*<br>Протокол № от 2021 года<br>. |
| 1. Состав и содержание политики приобретения информационных систем.<br>2. Какие в настоящее время существуют подходы к созданию систем информационной безопасности в РФ?<br>3. Как провести описание сценариев инцидентов информационной безопасности?<br><br>Профессор, д.т.н. А.Минзов | | |

**Процедура проведения**

Экзамен проводится в письменной форме по билетам согласно программе экзамена

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

**1. Компетенция/Индикатор:** ИД-2$_{ОПК-1}$ Организовать управление информационной безопасностью

**Вопросы, задания**

1.Какие в настоящее время существуют подходы к созданию систем информационной безопасности в РФ? Дайте краткую характеристику и принципиальные отличия.
2.Перечислите последовательность организации защиты информации в государственных информационных системах.
3.Перечислите последовательность организации защиты информации в негосударственных информационных системах.
4.Особенности организации защиты информации в концепции Cobit 5.0 по сравнению с ГОСТ Р ИСО/МЭК 27001.
5.Назначение и краткое содержание политики СМИБ.
6.Что включает в себя концепция СМИБ? С какой целью она разрабатывается?
7.Назначение и краткое содержание политики СИБ. Как разделяются 2 политики СИБ и СМИБ ?
8.Как классифицируются документы, разрабатываемые в концепциях стандарта ГОСТ Р ИСО/МЭК 27001,27002, 27005 ?
9.Состав и содержание политики непрерывности бизнеса.
10.Состав и содержание политики приобретения, разработки и эксплуатации информационных систем.
11.Состав и содержание политики безопасности, связанная с персоналом.
12.Состав и содержание политики расследования инцидентов.
13.Состав и содержание политики физической безопасности и защиты от окружающей среды.
14.Состав и содержание политики безопасности услуг электронной торговли.
15.Состав и содержание политики соответствия.
16.Как оценить стоимость информационных активов?
17.Как оценить ущерб от реализации угроз информационной безопасности?
18.Как оценить возможность реализации уязвимости информационной системы?
19.Как оценить меру затрат на создание СМИБ?
20.Какие существуют методы вычисления интегральных метрик оценки рисков?
21.Как провести описание сценариев инцидентов информационной безопасности? Как и где использовать эти сценарии?
22.Методы моделирования плана обработки рисков и выстраивания их приоритетов по уровню опасности на основе стратегий управления рисками и их анализа.
23.Методы учета связей между рисками по угрозам, уязвимостям, активам и мерам защиты. Выявления агрегатов рисков.
24.Понятие стратегии управления рисками. Анализ стратегий.
25.Как выбирать метод обработки рисков? Какие при этом используются правила ?
26.Политика менеджмента коммуникаций и работ.
27.Политика управления доступом.
28.Политика защиты персональных данных.
29.Политика защиты коммерческой тайны.
30.Политика защиты банковской тайны.
31.Политика аудита ИБ.

32.Политика распределения ролей персонала.
33.Политика обучения персонала.
34.Политика повышения осведомленности персонала.
35.Сущность концепции защиты информации на основе цикла Деминга –Шухарта.
36.Модель уязвимостей в концепции ГОСТ Р ИСО/МЭК 27002.
37.Многофакторная модель управления рисками информационной безопасности: назначение, решаемые задачи, стратегии рисков и последовательность работы.
38.Понятие риск информационной безопасности. Составляющие риска. С какой целью используется управление СМИБ на основе рисков ?
39.Обработка рисков: виды обработки и правила выбора процессов обработки.
40.Аксиомы и правила, используемые при моделировании рисков.
41.Алгоритм моделирования рисков информационной безопасности.
42.С какой целью устанавливается контекст организации при моделировании рисков?
43.Какие критерии управления рисками используются?
44.Какие методы определения опасности рисков рекомендуются в ГОСТ Р ИСО/МЭК 27005?
45.Почему при защите персональных данных не используются модели рисков?

**Материалы для проверки остаточных знаний**

1.Владение может распространяться на:

Ответы:

a) процесс бизнеса;
b) определенный набор деятельностей;
c) прикладные программы;
d) определенное множество данных;
e) операционные системы;
f) офисные приложения;
g) базы знаний.

Верный ответ: a, b, c, d

2.Какие риски информационной безопасности не следует учитывать при работе со сторонними организациями^

Ответы:

a) средства обработки информации, необходимые сторонним организациям для доступа;
b) тип доступа к информации и средствам обработки информации, который будет предоставлен сторонним организациям
c) ценность и чувствительность используемой информации, ее критичность для операций бизнеса;
d) места отгрузки и погрузки оборудования;
e) персонал сторонней организации, участвующий в обработке информации организации;
f) правильность авторизации;
g) различные способы и меры и средства контроля и управления, применяемые сторонними организациями при хранении, обработке, передаче, совместном использовании и обмене информацией;
h) влияние непредоставления требуемого доступа сторонней организации и ввода или получения сторонней организацией неточной или ложной информации;
i) инструкции и процедуры принятия мер в отношении инцидентов информационной безопасности и возможных убытков, а также сроки и условия возобновления доступа сторонних организаций в случае инцидента информационной безопасности;
j) правовые и нормативные требования, а также договорные обязательства, значимые для сторонних организаций, которые необходимо принимать в расчет;
k) интересы государства.

Верный ответ: a, b, c, e, f, g, h, i, j

3.Защита активов, включает:

Ответы:

a) процедуры защиты активов организации, в том числе информацию и программное обеспечение, а также менеджмент известных уязвимостей;

b) процедуры для определения компрометации активов, например вследствие потери или модификации данных;

c) целостность;

d) ограничения на копирование и разглашение информации;

e) процедуры доступности;

f) процедуры резервирования.

Верный ответ: a, b, c, d, e, f

***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

*Оценка:* 2

*Описание характеристики выполнения знания:* Работа не выполнена или выполнена преимущественно неправильно

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

Оценка определяется по совокупности результатов текущего контроля успеваемости в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ» на основании семестровой и экзаменационной составляющих

**Для курсового проекта/работы:**

**3 семестр**

**Форма проведения: Защита КП/КР**

***I. Процедура защиты КП/КР***

Порядок защиты курсовой работы устанавливается кафедрой

***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

*Оценка:* 2
*Описание характеристики выполнения знания:* Работа не выполнена или выполнена преимущественно неправильно

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

Оценка за курсовую работу определяется в соответствии с Положением о балльно-рейтинговой системе для студентов НИУ «МЭИ»