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
Технологии обеспечения информационной безопасности объектов

Москва
2024

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Разработчик	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Баронов О.Р. Идентификатор: R90d76356-BaronovOR-7bf8fd7e	О.Р. Баронов

СОГЛАСОВАНО:

Руководитель образовательной программы	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Минзов А.С. Идентификатор: R17801759-MinzovAS-e8de8907	А.С. Минзов
Заведующий выпускающей кафедрой	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ» Сведения о владельце ЦЭП МЭИ Владелец: Невский А.Ю. 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-2 Способен разрабатывать технический проект системы (подсистемы, компонента системы) обеспечения информационной безопасности

ИД-1 Анализирует угрозы информационной безопасности объектов и разрабатывать методы противодействия им

2. ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности

ИД-2 Разрабатывает проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности, в том числе и на объектах энергетики с критической информационной инфраструктурой, использующих АСУ ТП

и включает:

для текущего контроля успеваемости:

Форма реализации: Выполнение задания

1. Практическое задание № 1. Тема: Моделирование структуры системы менеджмента информационной безопасности с использованием технологии IDEF0 (Отчет)
2. Практическое задание № 2. Тема: Комплексное решение по разработке функциональной модели СМИБ с использованием технологии IDEF0 и организационно-распорядительной документации по обеспечению информационной безопасности на объекте с КИИ (Отчет)

Форма реализации: Выступление (доклад)

1. Документирование и описание процесса СУИБ. Коллоквиум (Коллоквиум)
2. Общая структура управленческой работы по обеспечению информационной безопасности на уровне предприятия (Коллоквиум)
3. Основные компоненты системы менеджмента информационной безопасности. Область действия СУИБ. Политика СУИБ. Коллоквиум (Коллоквиум)
4. Планирование, реализация, проверка и совершенствование СУИБ. Коллоквиум ()

БРС дисциплины

2 семестр

Раздел дисциплины	Веса контрольных мероприятий, %						
	Индекс КМ:	КМ-1	КМ-1	КМ-2	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	4	8	8	12	15
Система менеджмента информационной безопасности объектов							

Тема 1. Система менеджмента информационной безопасности.		+				
Тема 2. Менеджмент информационной безопасности на уровне предприятия.		+				
Тема 3. Управление обеспечением информационной безопасности организации.	+					
Тема 4. Система управления информационной безопасностью.	+					
Тема 5. Процессный подход в рамках управления ИБ.				+		
Тема 6. Работа с процессами СУИБ организации.			+	+		
Разработка СМИБ объектов с использованием методологии IDEF						
Тема 7. Стратегии построения и внедрения СУИБ.					+	
Тема 8. Методология моделирования системы менеджмента информационной безопасности организации с использованием технологии IDEF0.					+	
Тема 9. Моделирование системы менеджмента информационной безопасности организации с использованием технологии IDEF0.					+	
Проектирование СМИБ объектов с критической информационной инфраструктурой						
Тема 10. Проектирование системы менеджмента информационной безопасности для объектов КИИ различной категории значимости с использованием технологии IDEF0.						+
Тема 11. Разработка организационно-распорядительной документации для объектов КИИ (значимых и незначимых) с использованием технологии IDEF0.						+
Тема 12. Разработка проектной, рабочей и эксплуатационной документации на СМИБ.						+
Вес КМ:	15	10	15	10	25	25

$Общая часть/Для промежуточной аттестации$

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-2	ИД-1$_{ОПК-2}$ Анализирует угрозы информационной безопасности объектов и разрабатывать методы противодействия им	Знать: методику разработки систем обеспечения информационной безопасности требования современных отечественных и международных стандартов, руководящих документов и других нормативных документов по организации защиты информации Уметь: разрабатывать системы менеджмента информационной безопасности производить анализ угроз информационной безопасности объектов	Общая структура управленческой работы по обеспечению информационной безопасности на уровне предприятия (Коллоквиум) Основные компоненты системы менеджмента информационной безопасности. Область действия СУИБ. Политика СУИБ. Коллоквиум (Коллоквиум) Планирование, реализация, проверка и совершенствование СУИБ. Коллоквиум Практическое задание № 1. Тема: Моделирование структуры системы менеджмента информационной безопасности с использованием технологии IDEF0 (Отчет)
ОПК-3	ИД-2$_{ОПК-3}$ Разрабатывает проекты организационно-распорядительных документов, бизнес-	Знать: технологию разработки документов при создании системы менеджмента	Документирование и описание процесса СУИБ. Коллоквиум (Коллоквиум) Практическое задание № 2. Тема: Комплексное решение по разработке функциональной модели СМИБ с использованием технологии IDEF0 и

	планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности, в том числе и на объектах энергетики с критической информационной инфраструктурой, использующих АСУ ТП	информационной безопасности объекта Уметь: – разрабатывать проекты организационно-распорядительных документов по информационной безопасности на объектах энергетики с критической информационной инфраструктурой	организационно-распорядительной документации по обеспечению информационной безопасности на объекте с КИИ (Отчет)

II. Содержание оценочных средств. Шкала и критерии оценивания

КМ-1. Основные компоненты системы менеджмента информационной безопасности. Область действия СУИБ. Политика СУИБ. Коллоквиум

Формы реализации: Выступление (доклад)
Тип контрольного мероприятия: Коллоквиум
Вес контрольного мероприятия в БРС: 15
Процедура проведения контрольного мероприятия: Самостоятельная разработка ответов на вопросы коллоквиума

Краткое содержание задания:
Подготовить ответы на вопросы коллоквиума и разработать презентацию доклада
Вопросы коллоквиума::
1. Специфические черты организации информационной безопасности;
2. Деятельность по обеспечению ИБ организации как процесс;
3. Определение управления ИБ организации;
4. Управление ИБ информационно-телекоммуникационных технологий организации;
5. Цель, основные функции и компоненты СУИБ;
6. Область действия СУИБ;
7. Документальное обеспечение СУИБ;
8. Политика СУИБ;
9. Поддержка СУИБ со стороны руководства организации.

Контрольные вопросы/задания:

Уметь: производить анализ угроз информационной безопасности объектов	1.Какие данные являются входными данными для процесса ОИБ? 2.Что является выходом (результатом) деятельности по ОИБ в организации? 3.В чем заключается циклический характер процесс управления ИБ организации? 4.Каковы требования нормативных документов предъявляемые к процессу управления ИБ информационно-телекоммуникационныхтехнологий (ИТТ). 5.Какие важнейшие компоненты в конкретной организации включает в себя СУИБ? 6.Какова область действия СУИБ согласно требований стандарта ГОСТ Р 27001? 7.Какие документы входят в документацию СУИБ? 8. Какие ключевые процессы СУИБ должна охватывать политика СУИБ. 9. Для чего необходима поддержка руководства организации при разработке СУИБ?

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-1. Общая структура управленческой работы по обеспечению информационной безопасности на уровне предприятия

Формы реализации: Выступление (доклад)
Тип контрольного мероприятия: Коллоквиум
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Самостоятельная разработка ответов на вопросы коллоквиума

Краткое содержание задания:
Подготовить ответы на вопросы коллоквиума и разработать презентацию доклада
Вопросы коллоквиума:
1. Модель управления информационной безопасностью;
2. Анализ и управление рисками;
3. Порядок использования политик, стандартов и руководств;
4. Предпосылки развития менеджмента в сфере информационной безопасности на уровне предприятий;
5. Общая структура управленческой работы по обеспечению информационной безопасности на уровне предприятия;
6. Формирование политики информационной безопасности на предприятии.

Контрольные вопросы/задания:

Знать: требования современных отечественных и международных стандартов, руководящих документов и других нормативных документов по организации защиты информации	1.Что называется менеджментом ИБ? 2.Понятие управления рисками? 3.Что понимается под высокоуровневым документом, предназначенный для обеспечения управления 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

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

КМ-2. Документирование и описание процесса СУИБ. Коллоквиум

Формы реализации: Выступление (доклад)
Тип контрольного мероприятия: Коллоквиум
Вес контрольного мероприятия в БРС: 15
Процедура проведения контрольного мероприятия: Самостоятельная разработка ответов на вопросы коллоквиума

Краткое содержание задания:
Подготовить ответы на вопросы коллоквиума и разработать презентацию доклада
Вопросы коллоквиума::
1. Процессы цикла PDCA в применении к процессам СУИБ;

Контрольные вопросы/задания:

Знать: технологию разработки документов при создании системы менеджмента информационной безопасности объекта	1.Какие основные процессы СУИБ являются целевыми видами деятельности? 2.Что понимается под идентификацией процессов СУИБ? 3.Какова цель документирования процессов СУИБ? 4.Дайте понятие документированной процедуры? 5.Какие основные разделы включает в себя документированная процедура?

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. Планирование, реализация, проверка и совершенствование СУИБ. Коллоквиум

Формы реализации: Выступление (доклад)
Тип контрольного мероприятия:
Вес контрольного мероприятия в БРС: 10
Процедура проведения контрольного мероприятия: Самостоятельная разработка ответов на вопросы коллоквиума

Краткое содержание задания:
Подготовить ответы на вопросы коллоквиума и разработать презентацию доклада
Вопросы коллоквиума::
1. Процессы цикла PDCA в применении к процессам СУИБ;
2. Планирование СУИБ;
3. Реализация СУИБ;
4. Проверка СУИБ;
5. Совершенствование СУИБ.

Контрольные вопросы/задания:

Знать: методику разработки систем обеспечения информационной безопасности	1. Что такое управление ИБ как процессный подход? 2.Что такое управление ИБ как процессный подход? 3.В чем заключается выполнение этапа «Реализации» цикла PDCA? 4.Что является целью при выполнении деятельности в рамках группы процессов «проверка» цикла PDCA? 5.Что включает в себя группа процессов «совершенствование» цикла PDCA?

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. Практическое задание № 1. Тема: Моделирование структуры системы менеджмента информационной безопасности с использованием технологии IDEF0

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25

Процедура проведения контрольного мероприятия: Самостоятельное выполнение практического задания

Краткое содержание задания:

Выполнить практическую разработку функциональной модели системы менеджмента информационной безопасности с использованием технологии IDEF0

Контрольные вопросы/задания:

Уметь: разрабатывать системы менеджмента информационной безопасности	1.Чем отличается внедрения процессов СУИБ по отдельности от внедрения в целом? 2. Какими возможностями должна обладать методология функционального моделирования СУИБ? 3.В чем заключается функциональная оптимизация СУИБ?

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. Практическое задание № 2. Тема: Комплексное решение по разработке функциональной модели СМИБ с использованием технологии IDEF0 и организационно-распорядительной документации по обеспечению информационной безопасности на объекте с КИИ

Формы реализации: Выполнение задания
Тип контрольного мероприятия: Отчет
Вес контрольного мероприятия в БРС: 25
Процедура проведения контрольного мероприятия: Самостоятельное выполнение практического задания

Краткое содержание задания:

Выполнить практическую разработку функциональной модели СМИБ с использованием технологии IDEF0 и организационно-распорядительной документации по обеспечению информационной безопасности на объекте с КИИ

Контрольные вопросы/задания:

Уметь: – разрабатывать проекты	1.Каков порядок разработка предложений по

организационно-распорядительных документов по информационной безопасности на объектах энергетики с критической информационной инфраструктурой	совершенствованию организационно-распорядительных документов по безопасности значимых объектов КИИ системой СМИБ? 2.Каков порядок планирования и разработки мероприятий СМИБ по обеспечению безопасности значимых объектов критической информационной инфраструктуры с использованием технологии IDEF0.

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

СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

2 семестр

Форма промежуточной аттестации: Экзамен

Пример билета

<table>
<tr><td>НИУ
«МЭИ»
ИнЭИ</td><td rowspan="3">ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

по дисциплине: Технологии обеспечения информационной безопасности
направление подготовки: 10.04.01
форма обучения: очная</td><td rowspan="3">Утверждаю:
Зав. каф. БИТ
А.Ю.Невский
Протокол кафедры
№
« » декабря 2021г.</td></tr>
<tr><td>Кафедра
БИТ</td></tr>
<tr><td>2021 год</td></tr>
<tr><td colspan="3">1. Какова структура направлений организационной деятельности в сфере информационной безопасности?
2. Дайте характеристику трех базовых принципов управления на которых основывается создание СУИБ.
3. Какими возможностями должна обладать методология функционального при практическом моделировании СМИБ?</td></tr>
</table>

Процедура проведения

Письменный экзамен

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

1. Компетенция/Индикатор: ИД-1$_{ОПК-2}$ Анализирует угрозы информационной безопасности объектов и разрабатывать методы противодействия им

Вопросы, задания

1.Модель управления информационной безопасностью
2. Анализ и управление рисками
3.Специфические черты организации информационной безопасности
4.Деятельность по обеспечению ИБ организации как процесс
5.Определение управления ИБ организации
6.Управление ИБ информационно-телекоммуникационных технологий организации
7.Цель, основные функции и компоненты СУИБ
8.Документальное обеспечение СУИБ
9.Политика СУИБ
10. Подходы построения СУИБ
11.Построение и внедрение процессов СУИБ по отдельности
12.Постановка задачи построения функциональной SADTмодели СУИБ по семейству стандартов ISO/IEC 2700x
13.Методология функционального моделирования СМИБ
14.Функциональная модель системы защиты информации

Материалы для проверки остаточных знаний

1.Что называется менеджментом ИБ?

Ответы:

-

Верный ответ: Скоординированные действия, выполняемые с целью повышения и поддержания на требуемом уровне ИБ организации, называются менеджментом (организационно-техническим управлением) ИБ.

2.Какие два основных уровня управления в концептуальном плане включает в себя СМИБ?

Ответы:

-

Верный ответ: В концептуальном плане СМИБ включает в себя два основных уровня управления: - процедурный, касающийся документального оформления бизнес-процессов организации (процедурный уровень основывается на процессном подходе бизнес-риска, его цель состоит в создании, реализации, эксплуатации, мониторинге, анализе, повышении и поддержке заданного уровня ИБ); - организационно-технический, касающийся непосредственно мер безопасности (меры из стандартов ISO 27001-114 мер и NIST 800-53).

3.Понятие управления рисками?

Ответы:

-

Верный ответ: Управление рисками представляет собой процесс всестороннего изучения факторов, которые могут привести к реализации возможных угроз по отношению к активам информационной системы, для последующего выбора, реализации и контроля экономически эффективных мер безопасности.

4.Что включает в себя управление рисками в общем виде?

Ответы:

-

Верный ответ: Управление рисками включает в себя оценку риска, обработку риска, контроль и оптимизацию рисков. Процесс оценки рисков включает в себя два этапа: анализ рисков и оценивание рисков.

5.На что направлено управление информационной безопасностью на уровне предприятий?

Ответы:

-

Верный ответ: На уровне предприятий управление информационной безопасностью направлено на нейтрализацию различных видов внутренних и внешних угроз.

6.Какие специфические черты и присущи в современных условиях организации информационной безопасности?

Ответы:

-

Верный ответ: В современных условиях ОИБ присущи специфические черты: 1. Прогнозный характер проблем и задач в области ОИБ. 2. Деградация мер и средств, обеспечивающих ИБ. 3.Изменчивость (стохастичность) бизнеса. 4. Рост масштабов и сложности самих задач ОИБ организации. 5. Своевременность обнаружения проблем в области ОИБ.

7.Что является главным предназначением деятельности по организации информационной безопасности (ОИБ) организации?

Верный ответ: Главное предназначение деятельности по ОИБ организации – содействие основным, управленческим и иным вспомогательным процессам ведения бизнеса.

8.Дайте определение управления ИБ?

Ответы:

-

Верный ответ: Управление ИБ – это тоже процесс, представляющий собой логически взаимосвязанную между собой и непрерывную во времени последовательность работ, направленную на достижение поставленной специфичной цели ОИБ.

9.Что является целью разработки функциональной модели СУИБ.

Ответы:

-

Верный ответ: Целью разработки функциональной модели деятельности СУИБ является функциональная оптимизация деятельности СУИБ под потребности организации.

2. Компетенция/Индикатор: ИД-2$_{ОПК-3}$ Разрабатывает проекты организационно-распорядительных документов, бизнес-планов в сфере профессиональной деятельности, технической и эксплуатационной документации на системы и средства обеспечения информационной безопасности, в том числе и на объектах энергетики с критической информационной инфраструктурой, использующих АСУ ТП

Вопросы, задания

1.Задание процесса СУИБ
2.Идентификация процессов СУИБ организации
3.Документирование и описание процесса СУИБ
4.Мониторинг и измерение параметров процесса СУИБ
5.Система безопасности значимого объекта критической информационной инфраструктуры. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры
6.Функции СМИБ по ОБИ объекта КИИ. Разработка предложений по совершенствованию организационно-распорядительных документов по безопасности значимых объектов КИИ
7.Анализ угроз безопасности информации и выявление уязвимостей в отношении значимых объектов КИИ
8.Обеспечение реализации организационных мер и применение средств защиты информации, эксплуатацию средств защиты информации. Реагирование на компьютерные инциденты
9.Оценка соответствия значимых объектов КИИ требованиям по безопасности
10.Разработка предложений по совершенствованию функционирования систем безопасности, а также по повышению уровня безопасности значимых объектов критической информационной инфраструктуры
11.Моделирование комплексного решения по разработке функциональной модели СМИБ объектов КИИ с использованием технологии IDEF0
12.Планирование и разработка мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры
13.Реализация (внедрение) мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры
14.Контроль состояния безопасности значимых объектов критической информационной инфраструктуры
15.Совершенствование безопасности значимых объектов критической информационной инфраструктуры

Материалы для проверки остаточных знаний

1.Что такое управление ИБ как процессный подход?

Ответы:

-

Верный ответ: К управлению ИБ применим процессный подход, который распространяется на разработку, реализацию, эксплуатацию, мониторинг, анализ, сопровождение и совершенствование СУИБ организации. Поддержание на должном уровне СУИБ требует применения такого же подхода, как и любая другая система управления. Используемая в ISO/IEC 27001 и ГОСТ Р ИСО/МЭК 27001 для описания процессов СУИБ циклическая модель PDCA предусматривает непрерывный цикл мероприятий: «планирование – реализация – проверка – совершенствование». При таком подходе к управлению ИБ особое значение придается следующему: • пониманию требований по ОИБ организации и необходимости определить политику и цели ОИБ; • внедрению и использованию обоснованных защитных мер для управления рисками ИБ организации в контексте общих бизнесрисков организации; • мониторингу и анализу результативности и эффективности СУИБ; • постоянному совершенствованию, основанному на объективных показателях.

2.Что является целью деятельности в рамках группы процессов «планирование» цикла PDCA? Что такое управление ИБ как процессный подход?

Ответы:

-

Верный ответ: Целью выполнения деятельности в рамках группы процессов «планирование» является запуск цикла СУИБ путем определения первоначальных планов ее построения, ввода в действие и контроля, а также определения планов по совершенствованию на основании решений, принятых на этапе «Совершенствование».

3.В чем заключается выполнение этапа «Реализации» цикла PDCA?

Ответы:

-

Верный ответ: Этап «Реализация» осуществляется по результатам выполнения этапов «Планирование» и/или «Совершенствование» и заключается в выполнении всех планов, связанных с построением, вводом в действие и совершенствованием СУИБ, определенных на этапе планирования, и/или реализации решений, определенных на этапе совершенствования и не требующих выполнения деятельности по планированию соответствующих улучшений. Среди прочего важным является выполнение таких видов деятельности, как организация обучения и повышение осведомленности в области ИБ, реализация обнаружения и реагирования на инциденты ИБ, ОНБ.

4.Что является целью при выполнении деятельности в рамках группы процессов «проверка» цикла PDCA?

Ответы:

-

Верный ответ: Целью выполнения деятельности в рамках группы процессов «проверка» является обеспечение достаточной уверенности в том, что СУИБ, включая защитные меры, функционирует надлежащим образом и адекватна существующим угрозам ИБ, а также внутренним и/или внешним условиям функционирования организации, влияющим на ИБ. Кроме того, необходимо рассмотреть любые изменения в допущениях или области оценки рисков ИБ. Организация должна своевременно обнаруживать проблемы, прямо или косвенно относящиеся к ИБ, потенциально способные повлиять на ее бизнес-цели. Рекомендуется выявлять причинно-следственную связь возможных проблем и строить на этой основе прогноз их развития. Указанная деятельность может проводиться в любое время и с любой частотой, в зависимости от того, что является подходящим для конкретной ситуации. На этапе «Проверка» необходимо осуществлять мониторинг и контроль используемых защитных мер, проводить аудит

ИБ (внутренний и внешний), анализировать функционирование СУИБ в целом, в том числе со стороны руководства. Желательно интегрировать процессы мониторинга и анализа СУИБ в систему внутреннего контроля организации.

5.Что включает в себя группа процессов «совершенствование» цикла PDCA?

Ответы:

-

Верный ответ: Группа процессов «совершенствование» включает в себя деятельность по принятию решений о реализации тактических и/или стратегических улучшений СУИБ. Переход к этому этапу осуществляется только тогда, когда выполнение процессов этапа «Проверка» дало результат, требующий совершенствования СУИБ. При этом сама деятельность по совершенствованию СУИБ должна реализовываться в рамках групп процессов «реализация» (например, введение в действие существующего плана ОНБ, поскольку на стадии проверки определена необходимость в этом) и при необходимости – «планирование» (идентификация новой угрозы ИБ и последующие обновления оценки рисков на стадии планирования). При этом важно, чтобы все заинтересованные стороны немедленно извещались о проводимых улучшениях СУИБ и при необходимости проводилось соответствующее обучение.

6.Какие основные процессы СУИБ являются целевыми видами деятельности?

Ответы:

-

Верный ответ: Основными процессами СУИБ являются: • управление активами; • управление рисками ИБ; • управление инцидентами ИБ; • управление ролями, выполняемыми сотрудниками в рамках ОИБ; • управление персоналом, включая службу ИБ; • управление изменениями, улучшениями (тактическими, стратегическими), корректирующими и предупреждающими действиями; • управление защитными мерами; • управление информированием и обучением вопросам ОИБ; • управление документами и записями, относящимися к деятельности в области ОИБ в рамках СУИБ; • УНБ; • управление контрольными мероприятиями в области проверки уровня ИБ (мониторинг, внутренние и внешние аудиты ИБ); • управление эффективностью деятельности в области ОИБ.

7.Что понимается под идентификацией процессов СУИБ?

Ответы:

-

Верный ответ: Под идентификацией процессов СУИБ понимают определение состава процессов СУИБ, имеющих ключевое значение в рамках выбранной области действия – ОИБ, и составление их перечня, а также разработку модели каждого процесса, включающей краткую характеристику (например, в форме идентификационной карты), последовательность действий и процедуры процесса (например, в виде блок-схемы), показатели для оценки процесса.

8.Какова цель документирования процессов СУИБ?

Ответы:

-

Верный ответ: Цель документирования процессов СУИБ – описание их текущего состояния, что является первым шагом к их совершенствованию.

9.Какие этапы включает в себя процесс оценивания процессов СУИБ?

Ответы:

-

Верный ответ: Процесс оценивания ИБ включает следующие этапы: 1) определение входных данных: назначение, область действия, ограничения (по времени, доступности и т. п.), особенности, подход, критерии компетентности специалиста по оценке; 2) определение основных ролей и обязанностей; 3) представление

руководств для планирования, сбора данных, проверки их достоверности, определения атрибутов процесса и сообщения результатов оценки; 4) фиксирование выходных данных оценки.

10.1. Каковы основные подходя построения СУИБ?

Ответы:

-

Верный ответ: Существует два основных подхода построения СУИБ: • построение и внедрение СУИБ в целом; • построение и внедрение процессов управления ИБ по отдельности с последующим объединением их в единую СУИБ.

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