Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Самарский государственный экономический университет»

Институт Институт экономики предприятий

Кафедра Прикладной информатики

УТВЕРЖДЕНО
Ученым советом Университета
(протокол № 9 от 31 мая 2022 г.)

РАБОЧАЯ ПРОГРАММА

Наименование дисциплины Б1.В.18 Управление информационными проектами реализации комплексной безопасности

Основная профессиональная образовательная программа 09.03.03 Прикладная информатика программа Прикладная информатика и защита информации

Квалификация (степень) выпускника Бакалавр

Самара 2022

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Самарский государственный экономический университет»

Институт Институт экономики предприятий

Кафедра Прикладной информатики

АННОТАЦИЯ

Наименование дисциплины	Б1.В.18 Управление информационными проектами реализации комплексной безопасности
Основная профессиональная образовательная программа	09.03.03 Прикладная информатика программа Прикладная информатика и защита информации

Самара 2022

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Самарский государственный экономический университет»

Институт Институт экономики предприятий

Кафедра Прикладной информатики

УТВЕРЖДЕНО
Ученым советом Университета
(протокол № 9 от 31 мая 2022 г.)

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Наименование дисциплины	Б1.В.18 Управление информационными проектами реализации комплексной безопасности
Основная профессиональная образовательная программа	09.03.03 Прикладная информатика программа Прикладная информатика и защита информации

Самара 2022

Содержание (рабочая программа)

Стр.

Содержание (ФОС)

Стр.

Целью изучения дисциплины является формирование результатов обучения, обеспечивающих достижение планируемых результатов освоения образовательной программы.

1. Место дисциплины в структуре ОП

Дисциплина Управление информационными проектами реализации комплексной безопасности входит в часть, формируемая участниками образовательных отношений блока Б1.Дисциплины (модули)

Предшествующие дисциплины по связям компетенций: Хранение, обработка и анализ данных, Вычислительные системы, сети и телекоммуникации, Основы алгоритмизации и программирования, Основы проектной деятельности, Современные технологии и языки программирования, Проектирование и реализация баз данных, Теория информационной безопасности и методология защиты информации, Системы искусственного интеллекта, Облачные технологии и услуги, Технологии защищенного документооборота, Моделирование процессов и систем, Организационная защита информации, Техническая защита информации, Программно-аппаратная защита информации, Компьютерная экспертиза, Безопасность Web-приложений, Безопасность мобильных приложений, Правовая защита информации, Криптографическая защита информации, Методы и средства защиты информации, Технологии работы в социальных сетях, Встроенные языки программирования, Организация вычислительных процессов

Последующие дисциплины по связям компетенций: Разработка профессиональных приложений, Цифровая культура в профессиональной деятельности

2. Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе

Изучение дисциплины Управление информационными проектами реализации комплексной безопасности в образовательной программе направлено на формирование у обучающихся следующих компетенций:

Профессиональные компетенции (ПК):

ПК-1 - Способен к обнаружению и идентификации инцидентов в процессе эксплуатации автоматизированной системы

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
ПК-1	ПК-1.1: Знать:	ПК-1.2: Уметь:	ПК-1.3: Владеть (иметь навыки):
	особенности инцидентов в процессе эксплуатации автоматизированной системы	обнаруживать и идентифицировать инциденты в процессе эксплуатации автоматизированной системы	навыками обнаружения и идентификации инцидентов в процессе эксплуатации автоматизированной системы

ПК-2 - Способен к оценке защищенности автоматизированных систем с помощью типовых программных средств

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
ПК-2	ПК-2.1: Знать:	ПК-2.2: Уметь:	ПК-2.3: Владеть (иметь навыки):
	особенности защиты автоматизированных систем с помощью типовых программных	оценивать защищенность автоматизированных систем с помощью типовых программных	навыками защищенности автоматизированных систем с помощью типовых программных средств

	средств	средств	

ПК-4 - Способен к анализу изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
ПК-4	ПК-4.1: Знать:	ПК-4.2: Уметь:	ПК-4.3: Владеть (иметь навыки):
	основные угрозы безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	навыками анализа изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации

3. Объем и виды учебной работы

Учебным планом предусматриваются следующие виды учебной работы по дисциплине:

Очная форма обучения

Виды учебной работы	Всего час/ з.е.
	Сем 7
Контактная работа, в том числе:	74.3/2.06
Занятия лекционного типа	36/1
Лабораторные работы (лабораторный практикум)	36/1
Индивидуальная контактная работа (ИКР)	0.3/0.01
Групповая контактная работа (ГКР)	2/0.06
Самостоятельная работа:	35.7/0.99
Промежуточная аттестация	34/0.94
Вид промежуточной аттестации: Экзамен	 Экз
Общая трудоемкость (объем части образовательной программы): Часы Зачетные единицы	144 4

заочная форма

Виды учебной работы	Всего час/ з.е.
	Сем 8
Контактная работа, в том числе:	6.3/0.18
Занятия лекционного типа	2/0.06
Лабораторные работы (лабораторный практикум)	2/0.06
Индивидуальная контактная работа (ИКР)	0.3/0.01
Групповая контактная работа (ГКР)	2/0.06
Самостоятельная работа:	103.7/2.88
Промежуточная аттестация	34/0.94
Вид промежуточной аттестации: Экзамен	 Экз
Общая трудоемкость (объем части образовательной программы): Часы Зачетные единицы	144 4

4. Содержание дисциплины

4.1. Разделы, темы дисциплины и виды занятий:

Тематический план дисциплины Управление информационными проектами реализации

комплексной безопасности представлен в таблице.

Разделы, темы дисциплины и виды занятий
Очная форма обучения

№ п/п	Наименование темы (раздела) дисциплины	Контактная работа				Самостоятельная работа	Планируемые результаты обучения в соотношении с результатами обучения по образовательной программе
		Лекции	Занятия семинарского типа: Лаборат. работы	ИКР	ГКР		
1.	Обоснование проекта в сфере информационной безопасности. Планирование проекта в области информационной безопасности.	18	18			20	ПК-1.1, ПК-1.2, ПК -1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК- 4.1, ПК-4.2, ПК-4.3
2.	Фазы исполнения и внедрения проекта в сфере информационной безопасности	18	18			15,7	ПК-1.1, ПК-1.2, ПК -1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК- 4.1, ПК-4.2, ПК-4.3
	Контроль	34					
	Итого	**36**	**36**	**0.3**	**2**	**35.7**	

заочная форма

№ п/п	Наименование темы (раздела) дисциплины	Контактная работа				Самостоятельная работа	Планируемые результаты обучения в соотношении с результатами обучения по образовательной программе
		Лекции	Занятия семинарского типа: Лаборат. работы	ИКР	ГКР		
1.	Обоснование проекта в сфере информационной безопасности. Планирование проекта в области информационной безопасности.	2				50	ПК-1.1, ПК-1.2, ПК -1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК- 4.1, ПК-4.2, ПК-4.3
2.	Фазы исполнения и внедрения проекта в сфере информационной безопасности		2			53,7	ПК-1.1, ПК-1.2, ПК -1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК- 4.1, ПК-4.2, ПК-4.3
	Контроль	34					
	Итого	**2**	**2**	0.3	2	**103.7**	

4.2 Содержание разделов и тем

4.2.1 Контактная работа

Тематика занятий лекционного типа

№п/п	Наименование темы (раздела) дисциплины	Вид занятия лекционного типа*	Тематика занятия лекционного типа
1.	Обоснование проекта в сфере информационной	лекция	Основные определения в проектном управлении

	безопасности. Планирование проекта в области информационной безопасности.	лекция	Инициация проекта
		лекция	Разработка содержания проекта
		лекция	Разработка расписания проекта
		лекция	
		лекция	Планирование рисков проекта в сфере информационной безопасности
		лекция	
		лекция	Планирование человеческих ресурсов проекта
		лекция	Планирование коммуникаций и управления конфигурацией в проекте
2.	Фазы исполнения и внедрения проекта в сфере информационной безопасности	лекция	Управление проектом на фазе проектирования
		лекция	
		лекция	
		лекция	
		лекция	Управление проектом на фазе внедрения
		лекция	
		лекция	
		лекция	
		лекция	Подведение итогов

*лекции и иные учебные занятия, предусматривающие преимущественную передачу учебной информации педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях, обучающимся

Тематика занятий семинарского типа

№п/п	Наименование темы (раздела) дисциплины	Вид занятия семинарского типа**	Тематика занятия семинарского типа
1.	Обоснование проекта в сфере информационной безопасности. Планирование проекта в области информационной безопасности.	лабораторные работы	Командные роли в управлении проектами
		лабораторные работы	Настройка среды проектирования. Создание проекта
		лабораторные работы	
		лабораторные работы	
		лабораторные работы	
		лабораторные работы	Календарное планирование
		лабораторные работы	
		лабораторные работы	Планирование ресурсов и создание назначений
		лабораторные работы	
2.	Фазы исполнения и внедрения проекта в сфере информационной безопасности	лабораторные работы	Управление проектом
		лабораторные работы	
		лабораторные работы	
		лабораторные работы	
		лабораторные работы	
		лабораторные работы	
		лабораторные работы	
		лабораторные работы	Подведение итогов управления проектом
		лабораторные работы	

** семинары, практические занятия, практикумы, лабораторные работы, коллоквиумы и иные аналогичные занятия

Иная контактная работа

При проведении учебных занятий СГЭУ обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, проводимых организацией, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Формы и методы проведения иной контактной работы приведены в Методических указаниях по основной профессиональной образовательной программе.

4.2.2 Самостоятельная работа

№п/п	Наименование темы (раздела) дисциплины	Вид самостоятельной работы ***
1.	Обоснование проекта в сфере информационной безопасности. Планирование проекта в области информационной безопасности.	- подготовка доклада - подготовка электронной презентации - тестирование
2.	Фазы исполнения и внедрения проекта в сфере информационной безопасности	- подготовка доклада - подготовка электронной презентации - тестирование

*** самостоятельная работа в семестре, написание курсовых работ, докладов, выполнение контрольных работ

5. Материально-техническое и учебно-методическое обеспечение дисциплины

5.1 Литература:

Основная литература

1. Чекмарев, А. В. Управление ИТ-проектами и процессами : учебник для вузов / А. В. Чекмарев. — Москва : Издательство Юрайт, 2022. — 228 с. — (Высшее образование). — ISBN 978-5-534-11191-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493916

2.Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497002

Дополнительная литература:

1.Волкова, В. Н. Теория информационных процессов и систем : учебник и практикум для вузов / В. Н. Волкова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 432 с. — (Высшее образование). — ISBN 978-5-534-05621-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489220

2.Управление программными проектами : учебное пособие для вузов / В. Е. Гвоздев [и др.] ; под редакцией Р. Ф. Маликова. — Москва : Издательство Юрайт, 2022. — 167 с. — (Высшее образование). — ISBN 978-5-534-14329-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496651

3.Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496741

5.2. Перечень лицензионного программного обеспечения

1. Microsoft Windows 10 Education / Microsoft Windows 7 / Windows Vista Business

2. Office 365 ProPlus, Microsoft Office 2019, Microsoft Office 2016 Professional Plus (Word, Excel, Access, PowerPoint, Outlook, OneNote, Publisher) / Microsoft Office 2007 (Word, Excel, Access, PowerPoint)

5.3 Современные профессиональные базы данных, к которым обеспечивается доступ обучающихся

1. Профессиональная база данных «Информационные системы Министерства экономического развития Российской Федерации в сети Интернет» (Портал «Официальная Россия» - http://www.gov.ru/)

2. Профессиональная база данных «Финансово-экономические показатели Российской Федерации» (Официальный сайт Министерства финансов РФ - https://www.minfin.ru/ru/)

3. Профессиональная база данных «Официальная статистика» (Официальный сайт Федеральной службы государственной статистики - http://www.gks.ru/)

5.4. Информационно-справочные системы, к которым обеспечивается доступ обучающихся

1. Справочно-правовая система «Консультант Плюс»
2. Справочно-правовая система «ГАРАНТ-Максимум»

5.5. Специальные помещения

Учебные аудитории для проведения занятий лекционного типа	Комплекты ученической мебели Мультимедийный проектор Доска Экран
Учебные аудитории для проведения практических занятий (занятий семинарского типа)	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Учебные аудитории для групповых и индивидуальных консультаций	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Учебные аудитории для текущего контроля и промежуточной аттестации	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Помещения для самостоятельной работы	Комплекты ученической мебели Мультимедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ
Помещения для хранения и профилактического обслуживания оборудования	Комплекты специализированной мебели для хранения оборудования

5.6 Лаборатории и лабораторное оборудование

Лаборатория информационных технологий в профессиональной деятельности	Комплекты ученической мебели Мульмедийный проектор Доска Экран Компьютеры с выходом в сеть «Интернет» и ЭИОС СГЭУ Лабораторное оборудование

6. Фонд оценочных средств по дисциплине Управление информационными проектами реализации комплексной безопасности:

6.1. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля	Отметить нужное знаком « + »
Текущий контроль	Оценка докладов	-
	Устный/письменный опрос	-
	Тестирование	+
	Практические задачи	-
	Оценка контрольных работ (для заочной формы обучения)	+
Промежуточный контроль	Экзамен	+

Порядок проведения мероприятий текущего и промежуточного контроля определяется Методическими указаниями по основной профессиональной образовательной программе высшего образования, утвержденными Ученым советом ФГАОУ ВО СГЭУ, протокол № 9 от 31.05.2022; Положением о балльно-рейтинговой системе оценки успеваемости обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном автономном образовательном учреждении высшего образования «Самарский государственный экономический университет».

6.2. Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов обучения по программе

Профессиональные компетенции (ПК):

ПК-1 - Способен к обнаружению и идентификации инцидентов в процессе эксплуатации автоматизированной системы

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	ПК-1.1: Знать:	ПК-1.2: Уметь:	ПК-1.3: Владеть (иметь навыки):
	особенности инцидентов в процессе эксплуатации автоматизированной системы	обнаруживать и идентифицировать инциденты в процессе эксплуатации автоматизированной системы	навыками обнаружения и идентификации инцидентов в процессе эксплуатации автоматизированной системы
Пороговый	Теоретические аспекты комплексной системы защиты информации	классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности	Опытом работы с методами и моделями оценки эффективности комплексной системы защиты информации
Стандартный (в дополнение к пороговому)	Организационную структуру организации	Проводить аттестационные мероприятия	Опытом оценки эффективности защиты информации
Повышенный (в дополнение к пороговому, стандартному)	виды моделей, описывающих процессы защиты информации	формировать комплекс мер по защите информации на предприятии	Навыками разработки методических положений

ПК-2 - Способен к оценке защищенности автоматизированных систем с помощью типовых программных средств

Планируемые результаты обучения по	**Планируемые результаты обучения по дисциплине**

программе			
	ПК-2.1: Знать:	ПК-2.2: Уметь:	ПК-2.3: Владеть (иметь навыки):
	особенности защиты автоматизированных систем с помощью типовых программных средств	оценивать защищенность автоматизированных систем с помощью типовых программных средств	навыками защищенности автоматизированных систем с помощью типовых программных средств
Пороговый	основные причины, виды, каналы утечки и искажения информации	использовать соответствующие методы обеспечения информационной безопасности выбранных объектов	Навыками разработки документации для решения задач информационной безопасности
Стандартный (в дополнение к пороговому)	Архитектуру подсистем защиты информации в операционных системах	Проводить мониторинг функционирования программно-аппаратных средств защиты информации в операционных системах	Навыками управления антивирусной защитой операционных систем в соответствии с действующими требованиями
Повышенный (в дополнение к пороговому, стандартному)	Порядок обеспечения безопасности при эксплуатации программного обеспечения	Анализировать функционирование программного обеспечения с целью определения возможного вредоносного воздействия	Навыками формулирования требований к параметрам средств антивирусной защиты для корректной работы программного обеспечения

ПК-4 - Способен к анализу изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	ПК-4.1: Знать:	ПК-4.2: Уметь:	ПК-4.3: Владеть (иметь навыки):
	основные угрозы безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	анализировать изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации	навыками анализа изменения угроз безопасности информации автоматизированной системы, возникающих в ходе ее эксплуатации
Пороговый	Особенности управления информационной безопасностью, оценки рисков информационных ресурсов организации и аудита информационной безопасности	управлять информационной безопасностью, оценивать риски информационных ресурсов организации и аудита информационной безопасности	навыками управления информационной безопасностью, оценки рисков информационных ресурсов организации и аудита информационной безопасности
Стандартный (в дополнение к пороговому)	Особенности организации работы и разграничения полномочий персонала, ответственного за информационную безопасность	организовывать работу и разграничивать полномочия персонала, ответственного за информационную безопасность	навыками организации работы и разграничения полномочий персонала, ответственного за информационную безопасность

Повышенный (в дополнение к пороговому, стандартному)	Особенности формирования представления о содержании процессов управления информационной безопасностью организации как результата внедрения системного подхода к решению задач обеспечения информационной безопасности	формировать представления о содержании процессов управления информационной безопасностью организации как результата внедрения системного подхода к решению задач обеспечения информационной безопасности	навыками формирования представления о содержании процессов управления информационной безопасностью организации как результата внедрения системного подхода к решению задач обеспечения информационной безопасности

6.3. Паспорт оценочных материалов

№ п/п	Наименование темы (раздела) дисциплины	Контролируемые планируемые результаты обучения в соотношении с результатами обучения по программе	Вид контроля/используемые оценочные средства	
			Текущий	Промежуточный
1.	Обоснование проекта в сфере информационной безопасности. Планирование проекта в области информационной безопасности.	ПК-1.1, ПК-1.2, ПК- 1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК-4.1, ПК- 4.2, ПК-4.3	Тестирование Оценка контрольных работ (для заочной формы обучения)	Экзамен
2.	Фазы исполнения и внедрения проекта в сфере информационной безопасности	ПК-1.1, ПК-1.2, ПК- 1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК-4.1, ПК- 4.2, ПК-4.3	Тестирование Оценка контрольных работ (для заочной формы обучения)	Экзамен

6.4.Оценочные материалы для текущего контроля

Задания для тестирования по дисциплине для оценки сформированности компетенций (min 20, max 50 + ссылку на ЭИОС с тестами) https://lms2.sseu.ru/course/index.php?categoryid=1918

1. Кто является основным ответственным за определение уровня классификации информации?

A. Руководитель среднего звена
B. Высшее руководство
C. Владелец
D. Пользователь

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

A. Сотрудники
B. Хакеры
C. Атакующие

D. Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

A. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
B. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
C. Улучшить контроль за безопасностью этой информации
D. Снизить уровень классификации этой информации

4. Что самое главное должно продумать руководство при классификации данных?

A. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
B. Необходимый уровень доступности, целостности и конфиденциальности
C. Оценить уровень риска и отменить контрмеры
D. Управление доступом, которое должно защищать данные

5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

A. Владельцы данных
B. Пользователи
C. Администраторы
D. Руководство

6. Что такое процедура?

A. Правила использования программного и аппаратного обеспечения в компании
B. Пошаговая инструкция по выполнению задачи
C. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах
D. Обязательные действия

7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

A. Поддержка высшего руководства
B. Эффективные защитные меры и методы их внедрения
C. Актуальные и адекватные политики и процедуры безопасности
D. Проведение тренингов по безопасности для всех сотрудников

8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

A. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
B. Когда риски не могут быть приняты во внимание по политическим соображениям
C. Когда необходимые защитные меры слишком сложны
D. Когда стоимость контрмер превышает ценность актива и потенциальные потери

9. Что такое политики безопасности?

A. Пошаговые инструкции по выполнению задач безопасности

B. Общие руководящие требования по достижению определенного уровня безопасности
C. Широкие, высокоуровневые заявления руководства
D. Детализированные документы по обработке инцидентов безопасности

10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

A. Анализ рисков
B. Анализ затрат / выгоды
C. Результаты ALE
D. Выявление уязвимостей и угроз, являющихся причиной риска

11. Что лучше всего описывает цель расчета ALE?

A. Количественно оценить уровень безопасности среды
B. Оценить возможные потери для каждой контрмеры
C. Количественно оценить затраты / выгоды
D. Оценить потенциальные потери от угрозы в год

12. Тактическое планирование – это:

A. Среднесрочное планирование
B. Долгосрочное планирование
C. Ежедневное планирование
D. Планирование на 6 месяцев

13. Что является определением воздействия (exposure) на безопасность?

A. Нечто, приводящее к ущербу от угрозы
B. Любая потенциальная опасность для информации или систем
C. Любой недостаток или отсутствие информационной безопасности
D. Потенциальные потери от угрозы

14. Эффективная программа безопасности требует сбалансированного применения:

A. Технических и нетехнических методов
B. Контрмер и защитных механизмов
C. Физической безопасности и технических средств защиты
D. Процедур безопасности и шифрования

15. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

A. Внедрение управления механизмами безопасности
B. Классификацию данных после внедрения механизмов безопасности
C. Уровень доверия, обеспечиваемый механизмом безопасности
D. Соотношение затрат / выгод

16. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

A. Только военные имеют настоящую безопасность

B. Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
C. Военным требуется больший уровень безопасности, т.к. их риски существенно выше
D. Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

17. Как рассчитать остаточный риск?

A. Угрозы х Риски х Ценность актива
B. (Угрозы х Ценность актива х Уязвимости) х Риски
C. SLE х Частоту = ALE
D. (Угрозы х Уязвимости х Ценность актива) х Недостаток контроля

18. Что из перечисленного не является целью проведения анализа рисков?

A. Делегирование полномочий
B. Количественная оценка воздействия потенциальных угроз
C. Выявление рисков
D. Определение баланса между воздействием риска и стоимостью необходимых контрмер

19. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

A. Поддержка
B. Выполнение анализа рисков
C. Определение цели и границ
D. Делегирование полномочий

20. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

A. Чтобы убедиться, что проводится справедливая оценка
B. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
C. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа
D. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

Тематика контрольных работ

Раздел дисциплины	**Темы**
Обоснование проекта в сфере информационной безопасности. Планирование проекта в области информационной безопасности.	1. Характеристика различных определений проекта 2. Отличия жизненного цикла проекта от жизненного цикла продукта 3. Основные группы процессов управления проектом 4. Суть инициации проекта 5. SMART-цели проекта 6. Суть планирования проекта

	7. Методы, используемые при планировании проекта 8. Этапы разработки расписания проекта 9. Риски проекта в сфере информационной безопасности 10. Методы, используемые для снижения рисков проекта 11. Суть планирования человеческих ресурсов проекта 12. Системапланирования внутрифирменного проекта в сфере информационнойбезопасности. 13. Формирование и управление командой внутрифирменного проекта в сфере информационной безопасности. 14. Разработка концепции стратегии и бизнес-плана проекта в сфере информационнойбезопасности. 15. Сущность и проблемы управления проектами в сфере информационной безопасностина современном этапе. 16. Управление ресурсами проекта в кризисной ситуации. 17. Системный подход в управлении проектами в сфере информационной безопасности. 18. Управление рисками проекта в сфере информационной безопасности. 19. Проблемы управления стейкхолдерами в проектах обеспечивающих информационнуюбезопасность.
Фазы исполнения и внедрения проекта в сфере информационной безопасности	1. Методы формирования команды проекта 2. Виды коммуникаций, используемых в проекте 3. Суть управления конфигурацией проекта в сфере информационной безопасности 4. Причины корректировки фактического плана выполнения работ 5. Действия при управлении исполнения проекта 6. Суть процесса приемки результатов проекта 7. Типичные проблемы, возникающие в процессе приемки проектов в сфере информационной безопасности 8. История и перспективы развития управления проектами в сфере информационнойбезопасности в России. 9. Управление проектами обеспечивающих информационную безопасность в реальномсекторе экономики (на примере). 10. Управление проектами обеспечивающих информационную безопасность в сфереуслуг (на примере). 11. Управление проектами обеспечивающих информационную безопасность в банковском секторе экономики (на примере). 12. Управление проектами обеспечивающих информационную безопасность в социальной сфере (на примере). 13. Управление проектами обеспечивающих информационную безопасность в сфересвязей с общественностью (на примере).

6.5. Оценочные материалы для промежуточной аттестации

Фонд вопросов для проведения промежуточного контроля в форме экзамена

Раздел дисциплины	Вопросы
Обоснование проекта в сфере информационной безопасности. Планирование проекта в	1. Понятие проекта 2. Взаимосвязь управления проектами и и функционального менеджмента 3. Классификация типов проектов

области информационной безопасности.	4. Цель и стратегия проектов. Проектный цикл 5. Процессы управления проектом. 6. Стандарты управления проектами. Особенности российских стандартов (ГОСТ Р 54869—2011). 7. Модели жизненного цикла проекта. Соотношение жизненного цикла продукта ижизненного цикла проекта. 8. Организационная структура исполнителей проекта. Понятие функции, роли,должности. 9. Взаимоотношения «исполнитель-заказчик». Ключевые роли. Менеджер проекта.Примеры допустимого и недопустимого совмещения ролей для ИТ-проекта. 10. Инициация проекта. Определение целей и задач проекта. Формирование бизнес-целипроекта. 11. Критерии значимости проекта: финансовая и стратегическая ценность проекта,уровень рисков. 12. Идентификация окружения проекта: заинтересованные стороны проекта и анализ ихвоздействия на проект. Определение границ проекта. 13. Разработка устава проекта. Требования к структуре устава проекта. 14. Планирование проекта. Разработка базовых планов управления проектом. Видыпланов и их назначение. 15. Управление содержанием проекта и формирование иерархической структуры работ (ИСР) проекта. 16. Определение степени детализации ИСР. Формирование расписания проекта. 17. Ресурсы проекта. Закономерности распределения ресурсов. 18. Разработка расписания проекта. Метод критического пути. 19. Методы оценки стоимости проекта. Составление сметы проекта. Разработка базовогоплана по стоимости. 20. Идентификация и планирование управления рисками проекта. Понятие риска проекта, вероятности возникновения риска, оценка последствий риска, расчет величины риска.
Фазы исполнения и внедрения проекта в сфере информационной безопасности	1. Методы идентификации и приоритезации рисков. Наиболее распространенные рискипроектов в сфере информационной безопасности. 2. Методы качественного и количественного анализа рисков. Выработка стратегииреагирования на риски. 3. Управление исполнением и закрытие проекта. Мониторинг и контроль. Контролирующие показатели. 4. Управление сроками проекта и расписанием. Сбор данных о трудоемкости. 5. Текущий анализ состояния проекта. Анализ в контрольных точках. Анализ плановыхи фактических сроков и трудоемкости. 6. Метод освоенного объема. Мониторинг рисков проекта. 7. Регистрация и отслеживание ошибок. 8. Управление требованиями проекта. 9. Управление изменениями требований. 10. Спецификация и анализ влияния изменений.

	11. Управление конфигурацией. 12. Задачи и механизмы управления конфигурацией. 13. Средауправления конфигурацией. 14. Разработка плана управления конфигурацией. 15. Мониторинг состояния элементов конфигурации и аудиты. Управление изменениямии целостность элементов конфигурации. Матрица координации изменений. Журнал изменений проекта. 16. Этап закрытия проекта и его роль в обеспечении зрелости процессов проектногоуправления в организации. Анализ результатов проекта.

6.6. Шкалы и критерии оценивания по формам текущего контроля и промежуточной аттестации

Шкала и критерии оценивания

Оценка	**Критерии оценивания для мероприятий контроля с применением 4-х балльной системы**
«отлично»	Повышенный ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК- 4.1, ПК-4.2, ПК-4.3
«хорошо»	Стандартный ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК- 4.1, ПК-4.2, ПК-4.3
«удовлетворительно»	Пороговый ПК-1.1, ПК-1.2, ПК-1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК- 4.1, ПК-4.2, ПК-4.3
«неудовлетворительно»	Результаты обучения не сформированы на пороговом уровне