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 № 10 от 30 мая 2024 г.)

РАБОЧАЯ ПРОГРАММА

Наименование дисциплины Б1.В.16 Управление информационной безопасностью

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

Квалификация (степень) выпускника Бакалавр

Самара 2024

Содержание (рабочая программа)

Стр.

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

1. Место дисциплины в структуре ОП

Дисциплина Управление информационной безопасностью 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, Информационно-коммуникационные технологии в профессиональной деятельности, Встроенные языки программирования, Организация вычислительных процессов, Технологии работы в социальных сетях

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 информационной безопасностью 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-3 - Способен к составлению комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
ПК-3	ПК-3.1: Знать:	ПК-3.2: Уметь:	ПК-3.3: Владеть (иметь навыки):
	особенности составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе

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
Занятия семинарского типа	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

очно-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
Занятия семинарского типа	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 информационной безопасностью 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: Практич. занятия	ИКР	ГКР		
1.	Система управления информационной безопасностью	18	18	0,1		15	ПК-1.1, ПК-1.2, ПК -1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК- 3.1, ПК-3.2, ПК- 3.3, ПК-4.1, ПК- 4.2, ПК-4.3
2.	Аудит информационной безопасности. Средства поддержки процессов управления информационной безопасностью	18	18	0,2		35,7	ПК-1.1, ПК-1.2, ПК -1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК- 3.1, ПК-3.2, ПК- 3.3, ПК-4.1, ПК- 4.2, ПК-4.3
	Контроль	34					
	Итого	**36**	**36**	**0.3**	**2**	**35.7**	

очно-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: Практич. занятия	ИКР	ГКР		
1.	Система управления информационной безопасностью	1	1	0,15		50	ПК-1.1, ПК-1.2, ПК -1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК- 3.1,

							ПК-3.2, ПК- 3.3, ПК-4.1, ПК- 4.2, ПК-4.3
2.	Аудит информационной безопасности. Средства поддержки процессов управления информационной безопасностью	1	1	0,15		53,7	ПК-1.1, ПК-1.2, ПК -1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК- 3.1, ПК-3.2, ПК- 3.3, 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.	Система управления информационной безопасностью	лекция	Цели и задачи курса. Роль процесса управления
		лекция	Задачи процесса управления информационной безопасностью автоматизированных систем и организации в целом
		лекция	Задачи процесса управления информационной безопасностью автоматизированных систем и организации в целом (продолжение)
		лекция	Системный подход к управлению лекция информационной безопасностью.
		лекция	Системный подход к управлению лекция информационной безопасностью. (продолжение)
		лекция	Стандартизация в сфере управления информационной безопасностью
		лекция	Стандартизация в сфере управления информационной безопасностью (продолжение)
		лекция	Средства управления информационной безопасности
		лекция	Средства управления информационной безопасности (продолжение)
2.	Аудит информационной безопасности. Средства поддержки процессов управления информационной безопасностью	лекция	Назначение, цели и виды аудита ИБ. Требования к аудитору ИБ, особенности взаимодействия в процессе аудита
		лекция	Оценка работы аудитора. Стандартизация в сфере аудита информационной безопасности.
		лекция	Содержание и организация процесса аудита информационной безопасности.
		лекция	Оценка рисков информационной безопасности.
		лекция	Отчетные документы по результатам аудита. Выполнение рекомендаций по итогам проведения аудита

			информационной безопасности.
		лекция	Процессы управления информационной безопасностью. Процессно-ролевая модель
		лекция	Средства поддержки процессов управления информационной безопасностью
		лекция	Программные средства автоматизации процедур информационной безопасности и анализа политики информационной безопасности.
		лекция	Программные средства поддержки процессов управления информационной безопасности

*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.	Система управления информационной безопасностью	практическое занятие	Системный подход к управлению информационной безопасностью.
		практическое занятие	Системный подход к управлению информационной безопасностью. (продолжение)
		практическое занятие	Стандартизация в сфере управления информационной безопасностью
		практическое занятие	Стандартизация в сфере управления информационной безопасностью (продолжение)
		практическое занятие	Стандартизация в сфере управления информационной безопасностью (продолжение)
		практическое занятие	Средства управления информационной безопасности
		практическое занятие	Средства управления информационной безопасности (продолжение)
		практическое занятие	Средства управления информационной безопасности (продолжение)
		практическое занятие	Средства управления информационной безопасности (продолжение)
2.	Аудит информационной безопасности. Средства поддержки процессов управления информационной безопасностью	практическое занятие	Назначение, цели и виды аудита ИБ. Требования к аудитору ИБ, особенности взаимодействия в процессе аудита. Оценка работы аудитора. Стандартизация в сфере аудита информационной безопасности. Содержание и организация процесса аудита информационной безопасности. Оценка рисков информационной безопасности. Отчетные документы по результатам аудита. Выполнение рекомендаций по итогам проведения аудита информационной безопасности
		практическое занятие	Назначение, цели и виды аудита ИБ.

			Требования к аудитору ИБ, особенности взаимодействия в процессе аудита. Оценка работы аудитора. Стандартизация в сфере аудита информационной безопасности. Содержание и организация процесса аудита информационной безопасности. Оценка рисков информационной безопасности. Отчетные документы по результатам аудита. Выполнение рекомендаций по итогам проведения аудита информационной безопасности (продолжение)
		практическое занятие	Аудит информационной безопасности
		практическое занятие	Аудит информационной безопасности (продолжение)
		практическое занятие	Оценка рисков информационной безопасности
		практическое занятие	Оценка рисков информационной безопасности (продолжение)
		практическое занятие	Оценка рисков информационной безопасности (продолжение)
		практическое занятие	Средства поддержки процессов управления информационной безопасностью
		практическое занятие	Средства поддержки процессов управления информационной безопасностью (продолжение)

** 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.	Система управления информационной безопасностью	- подготовка доклада - подготовка электронной презентации - тестирование
2.	Аудит информационной безопасности. Средства поддержки процессов управления информационной безопасностью	- 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. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544029

2. Милешко, Л. П. Экономика и менеджмент безопасности : учебное пособие для вузов / Л. П. Милешко. — Москва : Издательство Юрайт, 2024. — 99 с. — (Высшее образование). — ISBN 978-5-534-13764-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/544007

Дополнительная литература

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2024. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536225

2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2024. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/539995

5.2. Перечень лицензионного программного обеспечения

1. Astra Linux Special Edition «Смоленск», «Орел»; РедОС
2. МойОфис Стандартный 2, МойОфис Образование, Р7-Офис Профессиональный

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. Государственная система правовой информации «Официальный интернет-портал правовой информации» (http://pravo.gov.ru/)
3. Профессиональная база данных «Финансово-экономические показатели Российской Федерации» (Официальный сайт Министерства финансов РФ - https://www.minfin.ru/ru/)
4. 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

6. Фонд оценочных средств по дисциплине Управление информационной безопасностью:

6.1. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля	Отметить нужное знаком « + »
Текущий контроль	Тестирование	+
	Оценка докладов	+
Промежуточный контроль	Экзамен	+

Порядок проведения мероприятий текущего и промежуточного контроля определяется Методическими указаниями по основной профессиональной образовательной программе высшего образования; 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	обнаруживать и идентифицировать инциденты в процессе	навыками обнаружения и идентификации инцидентов в процессе

	системы	эксплуатации автоматизированной системы	эксплуатации автоматизированной системы
Пороговый	особенности инцидентов	обнаруживать и идентифицировать инциденты	навыками обнаружения и идентификации инцидентов
Стандартный (в дополнение к пороговому)	особенности инцидентов в процессе эксплуатации автоматизированной системы	особенности инцидентов в процессе эксплуатации автоматизированной системы	навыками обнаружения и идентификации инцидентов в процессе эксплуатации автоматизированной системы
Повышенный (в дополнение к пороговому, стандартному)	особенности инцидентов в процессе эксплуатации автоматизированной системы и возможности не допущения инцидентов в процессе эксплуатации автоматизированной системы	особенности инцидентов в процессе эксплуатации автоматизированной системы и их обнаружение	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-2.1: 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	особенности защиты автоматизированных систем	оценивать защищенность автоматизированных систем	навыками защищенности автоматизированных систем
Стандартный (в дополнение к пороговому)	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
Повышенный (в дополнение к пороговому, стандартному)	особенности защиты автоматизированных систем с помощью дополнительных программных средств	оценивать защищенность автоматизированных систем с помощью дополнительных программных средств	навыками защищенности автоматизированных систем с помощью дополнительных программных средств

ПК-3 - Способен к составлению комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе

Планируемые результаты обучения по программе	**Планируемые результаты обучения по дисциплине**		
	ПК-3.1: Знать:	ПК-3.2: Уметь:	ПК-3.3: Владеть (иметь

			навыки):
	особенности составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе
Пороговый	особенности составления комплекса правил обеспечения защиты информации в автоматизированной системе	составлять комплекс правил обеспечения защиты информации в автоматизированной системе	навыками составления комплекса правил обеспечения защиты информации в автоматизированной системе
Стандартный (в дополнение к пороговому)	особенности составления комплекса правил, процедур, практических приемов, принципов и методов защиты информации в автоматизированной системе	составлять комплекс правила и процедуры практических приемов и методов защиты информации в автоматизированной системе	практическими приемами и методами обеспечения защиты информации
Повышенный (в дополнение к пороговому, стандартному)	особенности составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	составлять комплекс правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе	навыками составления комплекса правил, процедур, практических приемов, принципов и методов, средств обеспечения защиты информации в автоматизированной системе

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	Особенности	организовывать работу и	навыками организации

дополнение к пороговому)	организации работы и разграничения полномочий персонала, ответственного за информационную безопасность	разграничивать полномочия персонала, ответственного за информационную безопасность	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.	Система управления информационной безопасностью	ПК-1.1, ПК-1.2, ПК- 1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК-3.1, ПК- 3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-4.3	Тестирование	Экзамен
2.	Аудит информационной безопасности. Средства поддержки процессов управления информационной безопасностью	ПК-1.1, ПК-1.2, ПК- 1.3, ПК-2.1, ПК-2.2, ПК-2.3, ПК-3.1, ПК- 3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-4.3	Тестирование	Экзамен

6.4.Оценочные материалы для текущего контроля

Ссылка на текущую академическую активность, точки текущего контроля для всех оценочных материалов, размещенных в БРСО ЭИОС СГЭУ: https://lms2.sseu.ru/course/index.php?categoryid=1918

Примерная тематика докладов

Раздел дисциплины	Темы
Система управления информационной безопасностью	1. Управление информационной безопасностью. 2. Основные угрозы доступности. 3. Основные угрозы целостности. 4. Основные угрозы конфиденциальности. 5. «Оранжевая книга» как оценочный стандарт. 6. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем. 7. Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения.

	8. Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования". 9. Сертификация СУИБ на соответствие ISO 27001 10. Этапы разработки и внедрения системы управления ИБ. 11. Содержание этапов разработки и внедрения системы управления ИБ.
Аудит информационной безопасности. Средства поддержки процессов управления информационной безопасностью	1. Управление рисками. 2. Метод оценки рисков на основе модели угроз и уязвимостей 3. Расчет рисков по угрозе конфиденциальность 4. Расчет рисков по угрозе целостность 5. Качественные методики управления рисками. 6. Методики COBRA и RA Software Tool. 7. Количественные методики управления рисками. 8. Метод CRAMM. 9. Методы оценивания информационных рисков 10. Табличные методы оценки рисков 11. Методика FRAP. 12. Методика OCTAVE 13. Методика Risk Watch 14. Управление информационной безопасностью предприятия. 15. Основные программно-технические меры. 16. Идентификация и аутентификация. 17. Управление доступом.

Задания для тестирования по дисциплине для оценки сформированности компетенций (min 20, max 50 + ссылку на ЭИОС с тестами)

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

6.5. Оценочные материалы для промежуточной аттестации

Фонд вопросов для проведения промежуточного контроля в форме экзамена

Раздел дисциплины	Вопросы
Система управления информационной безопасностью	1. Понятие информационной безопасности 2. Основные составляющие информационной безопасности. 3. Управление информационной безопасностью.

	4. Важность и сложность проблемы информационной безопасности 5. Основные определения и критерии классификации угроз. 6. Основные угрозы доступности. 7. Основные угрозы целостности. 8. Основные угрозы конфиденциальности. 9. Вредительские программы 10. Роль стандартов ИБ. 11. «Оранжевая книга» как оценочный стандарт. 12. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем. 13. Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения. 14. Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования". 15. Сертификация СУИБ на соответствие ISO 27001 16. Этапы разработки и внедрения системы управления ИБ. 17. Содержание этапов разработки и внедрения системы управления ИБ.
Аудит информационной безопасности. Средства поддержки процессов управления информационной безопасностью	18. Управление рисками. Основные понятия. 19. Метод оценки рисков на основе модели угроз и уязвимостей 20. Расчет рисков по угрозе конфиденциальность 21. Расчет рисков по угрозе целостность 22. Качественные методики управления рисками. 23. Методики COBRA и RA Software Tool. 24. Количественные методики управления рисками. 25. Метод CRAMM. 26. Постановка задачи 27. Методы оценивания информационных рисков 28. Табличные методы оценки рисков 29. Методика анализа рисков Microsoft 30. Обоснование необходимости инвестиций в информационную безопасность компании. 31. Методика FRAP. 32. Методика OCTAVE 33. Методика Risk Watch 34. Обзор российского законодательства в области информационной безопасности 35. Закон "Об информации, информатизации и защите информации" 36. Другие законы и нормативные акты 37. О текущем состоянии российского законодательства в области информационной безопасности 38. Обзор зарубежного законодательства в области информационной безопасности 39. Общие положения организационной защиты. 40. Особенности организационной защиты компьютерных информационных систем и сетей. 41. Управление информационной безопасностью предприятия. 42. Основные программно-технические меры. 43. Идентификация и аутентификация. 44. Управление доступом.

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- 3.1, ПК-3.2, ПК-3.3, 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- 3.1, ПК-3.2, ПК-3.3, 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- 3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-4.3
«неудовлетворительно»	Результаты обучения не сформированы на пороговом уровне