ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Голлай А. В.
Пользователь: gollaiav
Дата подписания: 15.10.2021

А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины Б.1.43 Аудит информационной безопасности
для специальности 10.05.03 Информационная безопасность автоматизированных систем
уровень специалист **тип программы** Специалитет
специализация Информационная безопасность автоматизированных систем критически важных объектов
форма обучения очная
кафедра-разработчик Защита информации

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

Зав.кафедрой разработчика,
к.техн.н., доц.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 15.10.2021

А. Н. Соколов

Разработчик программы,
старший преподаватель

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Мищенко Е. Ю.
Пользователь: mishchenkoei
Дата подписания: 15.10.2021

Е. Ю. Мищенко

Челябинск

1. Цели и задачи дисциплины

Цель: освоение технологий аудита информационной безопасности организации. Задачи: - изучение базовых понятий, методов, технологий аудита информационной безопасности организации; - изучение отечественных и зарубежных стандартов, на основе которых осуществляется аудит информационной безопасности организации; - освоение программных средств для проведения аудита информационной безопасности организации.

Краткое содержание дисциплины

В рамках дисциплины изучаются: - базовые понятия, методы, технологии аудита информационной безопасности организации; - отечественные и зарубежные стандарты, на основе которых осуществляется аудит информационной безопасности организации; - программные средства для проведения аудита информационной безопасности организации.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУНы)
ПСК-3.5 способностью проектировать, внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов	Знать:типовые проектные решения по созданию систем обеспечения безопасности информации
	Уметь:контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем
	Владеть:методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем
ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Знать:базовые угрозы информационной безопасности
	Уметь:разрабатывать модели угроз информационной безопасности и модели нарушителя критически важных объектов информатизации
	Владеть:методиками определения актуальных угроз информационной безопасности
ПК-3 способностью проводить анализ защищенности автоматизированных систем	Знать:требования защиты информации к критически важным объектам информатизации
	Уметь:разрабатывать отчетную документацию по результатам обследования объекта информатизации
	Владеть:методиками проведения анализа защищенности объекта информатизации
ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	Знать:базовые угрозы информационной безопасности
	Уметь:разрабатывать протоколы инструментальных измерений параметров защищенности информации
	Владеть:навыками работы с техническими и

	программно-аппаратными средствами контроля защищенности
ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	Знать:типовые проектные решения по созданию систем обеспечения безопасности информации
	Уметь:разрабатывать рекомендации по совершенствованию системы защиты информации
	Владеть:методиками технико-экономического анализа мер по обеспечению безопасности информации
ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы	Знать:нормативные критерии определения ущерба при нарушении информационной безопасности
	Уметь:
	Владеть:методиками определения рисков информационной безопасности

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Б.1.30.01 Разработка защищенных автоматизированных систем, В.1.08 Основы аттестации объектов информатизации критически важных объектов	Не предусмотрены

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
Б.1.30.01 Разработка защищенных автоматизированных систем	Знания основных угроз безопасности информации и модели нарушителя в автоматизированных системах; основных мер по защите информации в автоматизированных системах (организационные, правовые, программно-аппаратные, криптографические, технические); основных криптографических методов, алгоритмов, протоколов, используемых для обеспечения информационной безопасности в автоматизированных и телекоммуникационных системах
В.1.08 Основы аттестации объектов информатизации критически важных объектов	Знания требований защиты информации к аттестованным объектам Навыки мониторинга изменения состояния аттестованного объекта

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч.

Вид учебной работы	Всего	Распределение

	часов	по семестрам в часах
		Номер семестра
		10
Общая трудоёмкость дисциплины	144	144
Аудиторные занятия:	72	72
Лекции (Л)	36	36
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	36	36
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	72	72
Проведение аудита информационной безопасности конкретной организации (объекта ВКР, по выбору студента, по заданию преподавателя)	72	72
Вид итогового контроля (зачет, диф.зачет, экзамен)	-	экзамен

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР
1	Аудит безопасности и методы его проведения	8	8	0	0
2	Оценка безопасности информационных технологий на основе «Общих критериев»	6	6	0	0
3	Оценка безопасности на основе Международного стандарта по управлению информационной безопасностью ISO 17799	6	6	0	0
4	Программные средства для проведения аудита информационной безопасности.	18	8	10	0
5	Методика проведения аудита информационной безопасности на предприятии	34	8	26	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Аудит безопасности и методы его проведения.Понятие аудита безопасности. Методы анализа данных при аудите ИБ. Понятие критически важного объекта. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (11.07.2012)	4
2	1	Анализ информационных рисков предприятия. Методы оценивания информационных рисков. Управление информационными рисками.	4
3	2	Стандарты информационной безопасности.Предпосылки создания стандартов ИБ. Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга). Гармонизированные критерии Европейских стран. Германский стандарт BS1. Британский стандарт BS 7799. Международный стандарт ISO 17799. Международный стандарт ISO 15408 «Общие критерии» . Стандарт COBIT. Стандарты по безопасности информационных технологий в России	4
4	2	Оценка безопасности информационных технологий на основе «Общих критериев» Предпосылки введения международного стандарта ISO 15408.	2

		Основные понятия общих критериев. Методология оценки безопасности информационных технологий по общим критериям.Оценка уровня доверия функциональной безопасности информационной технологии. Обзор классов и семейств ОК	
5	3	Международный стандарт управления информационной безопасностью ISO 17799Назначение стандарта ISO 17799 для управления информационной безопасностью. Практика прохождения аудита и получения сертификата ISO 17799.	4
6	3	Международный стандарт управления информационной безопасностью ISO 17799. Политика безопасности. Организационные меры по обеспечению информационной безопасности. Классификация ресурсов и их контроль. Безопасность персонала. Физическая безопасность. Администрирование компьютерных систем и вычислительных сетей. Управление доступом к системам. Разработка и сопровождение информационных систем. Планирование бесперебойной работы организации. Соответствие системы основным требованиям	2
7	4	Программные средства для проведения аудита информационной безопасности. Анализ видов используемых программных продуктов. Система CRAMM.	4
8	4	Программные средства для проведения аудита информационной безопасности. Система КОНДОР. Сетевые сканеры	4
9	5	Методика проведения аудита информационной безопасности на предприятии Три подхода к проведению аудита ИБ. Задачи и содержание работ при проведении аудита ИБ. Подготовка предприятий к проведению аудита ИБ. Планирование процедуры аудита ИБ. Организация и проведения работ по аудиту. Алгоритм проведения аудита безопасности предприятия.	4
10	5	Методика проведения аудита ИБ.Перечень и систематизация данных, необходимых для проведения аудита ИБ. Выработка рекомендаций и подготовка отчетных документов. Экономическая оценка обеспечения ИБ. Особенности аудита ИБ критически важных объектов	4

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	4	Сравнительный анализ программных средств для проведения аудита ИБ.	2
2	4	Система CRAMM.	2
3	4	Система КОНДОР.	2
4	4	Сетевые сканеры.	4
5	5	Методика проведения аудита информационной безопасности на предприятии.	4
6	5	Планирование процедуры аудита ИБ.	4
7	5	Организация и проведение работ по аудиту по Алгоритму проведения аудита безопасности предприятия.	4
8	5	Методика проведения аудита информационной безопасности на предприятии. Выработка рекомендаций.	4
9	5	Методика проведения аудита информационной безопасности на предприятии. Подготовка отчетных документов.	2
10	5	Экономическая оценка обеспечения ИБ и ее аудита.	2
11	5	Особенности аудита ИБ критически важных объектов.	4
12	5	Защита семестровых заданий по СРС.	2

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием разделов, глав, страниц)	Кол-во часов
Проведение аудита ИБ конкретной организации	Аверченков, В.И. Аудит информационной безопасности: Учебное пособие 2-е издание, стереотипное.- М.: Издательство «ФЛИНТА», 2011.-269с.	72

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
Проектная работа студентов	Практические занятия и семинары	Проведение аудита информационной безопасности конкретной организации (по выбору студента, объекта ВКР, по выбору преподавателя) в рамках проекта по комплексному анализу состояния защищенности объекта (предпроектное обследование, технический паспорт автоматизированной системы, текущее состояние защищенности, формирование рекомендаций по повышению эффективности средств защиты информации)	36

Собственные инновационные способы и методы, используемые в образовательном процессе

Не предусмотрены

Использование результатов научных исследований, проводимых университетом, в рамках данной дисциплины: нет

7. Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1. Паспорт фонда оценочных средств

Наименование разделов дисциплины	Контролируемая компетенция ЗУНы	Вид контроля (включая текущий)	№№ заданий
Аудит безопасности и методы его проведения	ПК-3 способностью проводить анализ защищенности автоматизированных систем	экзамен	1-3
Аудит безопасности и методы его проведения	ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы	экзамен	4-6,11-13

Оценка безопасности информационных технологий на основе «Общих критериев»	ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	экзамен	7-10
Оценка безопасности на основе Международного стандарта по управлению информационной безопасностью ISO 17799	ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	экзамен	7-10,23
Программные средства для проведения аудита информационной безопасности.	ПСК-3.5 способностью проектировать, внедрять и использовать системы мониторинга средств защиты информации, функционирующих на критически важных объектах и в автоматизированных системах критически важных объектов	экзамен	14-20
Программные средства для проведения аудита информационной безопасности.	ПК-17 способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	экзамен	21-22
Методика проведения аудита информационной безопасности на предприятии	ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	экзамен	24-27
Методика проведения аудита информационной безопасности на предприятии	ПК-5 способностью проводить анализ рисков информационной безопасности автоматизированной системы	экзамен	28-30
Методика проведения аудита информационной безопасности на предприятии	ПК-6 способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности	экзамен	31-34

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
экзамен	студенты в аудитории письменно отвечают на вопросы экзаменационного билета, который включает теоретические вопросы и задачи по пройденным разделам, преподаватель проверяет, беседует и оценивает	Отлично: обладает твёрдым и полным знанием материала дисциплины, владеет дополнительными знаниями, даны полные, развёрнутые ответы; логически, грамотно и точно излагает материал дисциплины, интерпретируя его самостоятельно, способен самостоятельно его анализировать и делать выводы. Хорошо: знает материал дисциплины в запланированном объёме, некоторые моменты в ответе не отражены или в ответе имеются несущественные неточности; грамотно и по существу излагает материал. Удовлетворительно: знает только основной материал дисциплины, не усвоил его деталей, дана только часть ответа на вопросы; в ответе имеются существенные ошибки; допускает неточности в изложении и интерпретации знаний; имеются нарушения логической последовательности в изложении материала. Неудовлетворительно: не знает значительной части

		материала дисциплины; ответ не дан или допускает грубые ошибки при изложении ответа на вопрос; неверно излагает и интерпретирует знания; изложение материала логически не выстроено.

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
экзамен	1. Базовые сведения о проверке и оценке уровня ИБ организации. 2. Проверки и оценки уровня ИБ организации. 3. Аудит ИБ организации: общие понятия и определения. 4. Виды аудита ИБ организации. 5. Принципы и формы аудита ИБ организации. 6. Профессиональная квалификация аудитора ИБ. 7. Стандарты проведения аудита ИБ. 8. Нормативы для проведения аудита ИБ организации. 9. Стандарты в области управления ИБ. 10. Стандарты управление рисками ИБ. 11. Методология аудита ИБ. 12. Организация процесса аудита ИБ. 13. Основные этапы и методы работ по проведению аудита ИБ. 14. Программа аудита ИБ. 15. Сбор свидетельств (исходной информации) для проведения аудита ИБ. 16. Рекомендации по планированию аудита ИБ. 17. Рекомендации по моделированию. 18. Рекомендации по тестированию. 19. Рекомендации по анализу и документированию результатов аудита ИБ. 20. Инструментальные средства аудита ИБ. 21. Методы и инструментальные средства проведения аудита ИБ. 22. Программные средства анализа и управления. 23. Основные разделы управления ИБ по стандарту ISO 17799. 24. Ключевые средства контроля контроля ИБ предприятия. 25. Политика информационной безопасности. Основные положения политики обеспечения информационной безопасности. 26. Организационные меры управления информационной безопасностью. 27. Классификация информационных ресурсов, уровни их защиты. 28. Обучение персонала вопросам, связанным с информационной безопасностью организации. Участие и роль персонала в процессах аудита ИБ. 29. Основные правила защиты центров данных и компьютерных залов. 30. Основные правила работы с носителями информации и их защитой. 31. Система CRAMM — назначение, достоинства и недостатки. 32. Концептуальная схема проведения обследования предприятия по методу CRAMM. 33. Назначение и принципы работы системы КОНДОР. 34. Сетевые сканеры. Цели функционирования, виды, назначение. Использование сетевых сканеров при аудите ИБ.

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

Не предусмотрена

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

1. Защита информации. Инсайд ,информ.-метод. журн. ,Изд. дом "Афина"
2. Защита информации. Конфидент / Ассоц. защиты информ. "Конфидент" : информ.-метод. журн
3. БДИ: Безопасность. Достоверность. Информация рос. журн. о безопасности бизнеса и личности ООО "Журн. "БДИ" журнал"
4. Безопасность информационных технологий ,12+ ,М-во образования и науки Рос. Федера-ции, Моск. инж.-физ. ин-т (гос. ун-т), ВНИИПВТИ
5. Вестник УрФО : Безопасность в информационной сфере ,Юж.-Урал. гос. ун-т; ЮУрГУ

г) методические указания для студентов по освоению дисциплины:

1. Аудит информационной безопасности

из них: учебно-методическое обеспечение самостоятельной работы студента:

1. Аудит информационной безопасности

Электронная учебно-методическая документация

№	Вид литературы	Наименование ресурса в электронной форме	Библиографическое описание
1	Основная литература	eLIBRARY.RU	Макаренко, С. И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями / С. И. Макаренко. – Санкт-Петербург : Издательство «Наукоемкие технологии», 2018. – 122 с. https://elibrary.ru/item.asp?id=36445362
2	Основная литература	eLIBRARY.RU	Кадыров, А. Р. Методы аудита информационной безопасности / А. Р. Кадыров, Н. А. Алтынбекова, А. Р. Жолдошбекова // Современные проблемы механики. – 2020. – № 39(1). – С. 63-72. https://elibrary.ru/item.asp?id=44801644
3	Дополнительная литература	eLIBRARY.RU	Хлестова, Д. Р. Аудит информационной безопасности в организации / Д. Р. Хлестова, Ф. Т. Байрушин // Символ науки: международный научный журнал. – 2016. – № 11-3(23). – С. 175-177. https://elibrary.ru/item.asp?id=27413109
4	Дополнительная литература	eLIBRARY.RU	Воеводин, В. А. Постановка задачи и обоснование выбора методов выборочного контроля при проведении аудита информационной безопасности / В. А. Воеводин, М. С. Оксина, Е. А. Фролова // REDS: Телекоммуникационные устройства и системы. – 2017. – Т. 7. – № 4. – С. 507-510. https://elibrary.ru/item.asp?id=30309243
5	Дополнительная литература	eLIBRARY.RU	Зелинская, Е. Л. Аудит безопасности информационных систем: виды и этапы работ / Е. Л. Зелинская, А. Г. Зелинский // Морская стратегия и политика России в контексте обеспечения национальной безопасности и устойчивого развития в XXI веке : Сборник научных трудов. – Севастополь : Черноморское высшее военно-морское

			ордена Красной Звезды училище им. П.С. Нахимова, 2019. – С. 165-169. https://elibrary.ru/item.asp?id=41203550

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

1. Microsoft-Windows(бессрочно)
2. Microsoft-Office(бессрочно)

Перечень используемых информационных справочных систем:

1. -Консультант Плюс(31.07.2017)

10. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лекции	912 (3б)	Комплект компьютерного оборудования, LCD Проектор, Экран проекционный, настенные стенды по защите информации (5 шт.), программное обеспечение: ОС Windows XP , MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+.
Практические занятия и семинары	913 (3б)	Комплект компьютерного оборудования; Локальная вычислительная сеть; Коммутатор, Программное обеспечение: ОС Windows 10, MS Office 2007, Matlab, WinRar, Mozila Firefox, Консультант+; Локальные СЗИ: Secret Net 6.5 (автономный вариант), Страж 3.0; Межсетевые экраны: ViPNet Custom 3.1, User Gate 5.2