



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.04.13 Аудит защищенности информационного объекта

Направление подготовки: 10.03.01 Информационная безопасность

Направленность (профиль): Организация и технология защиты информации (по отрасли или в сфере профессиональной деятельности)

Квалификация (степень): бакалавр

Форма обучения: очная

Институт: математики, естествознания и техники

Кафедра: математического моделирования, компьютерных технологий и информационной безопасности

	очная форма	очно-заочная форма	заочная форма
Курс	4		
Семестр	7,8		

Лекции	24		
Лабораторные занятия	34		
Практические (семинарские) занятия	24		
в т. ч. практическая подготовка	8		
Форма(ы) промежуточной аттестации	Зачет Экзамен-0,3		
Контроль	9		
Иные формы работы			
Самостоятельная работа	196,7		

Всего часов: 288

Трудоемкость: 8 зачетных единиц.

Разработчик(и) рабочей программы:
кандидат педагогических наук, доцент

Т.А. Щучка

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины:

- освоение компетенций по применению комплекса мероприятий в системе защиты информации на основе организации и проведения аудита защищенности информационного объекта.

Задачи изучения дисциплины:

- изучение основных понятий аудита защищенности информационного объекта;
- изучение процессного подхода к организации информационной безопасности;
- изучение основных требований к содержанию аудита защищенности информационного объекта;
- изучение основ контроля и проверки процессов и систем;
- изучение процесса комплексного обследования информационной безопасности; изучение методов оценивания информационной безопасности;
- формирование умений оценивания информационной безопасности на основе показателей информационной безопасности;
- формирование навыков использования методологии, стандартов и нормативных требований в области аудита защищенности информационного объекта.

Место дисциплины в структуре ОПОП: реализуется в части, формируемой участниками образовательных отношений блока Б1. Дисциплины (модули).

Планируемые результаты обучения по дисциплине:

Код компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК 2.4	Знать: - основные понятия, объекты и службы информационной безопасности, требования к объектам и средствам защиты информации; - этапы и процедуры комплексного аудита информационной безопасности защищённых автоматизированных систем.	Знает: - меры по обеспечению информационной безопасности и методы управления процессом их реализации на объекте защиты.
	Уметь: - осуществлять мероприятия комплексного аудита, оценивать состояние защищенности информации и соответствие объектов требованиям руководящих документов; - составлять нормативную и отчетную документацию по результатам проверки; анализировать результаты проверок и формулировать выводы по ним.	Умеет: - формировать политику информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности
	Владеть: - методами сбора и оценки соответствия свидетельств аудита информационной безопасности защищённых	Владеет: - навыками управления процессом реализации политики информационной безопасности, организации и

	автоматизированных систем нормативным требованиям по защите информации; - навыками оформления отчетной документации по результатам аудита объекта защиты.	поддержки выполнения комплекса мер по обеспечению информационной безопасности на объекте защиты.
--	--	--

II. СОДЕРЖАНИЕ И ОБЪЕМ ДИСЦИПЛИНЫ

с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу

Очная форма обучения

№	Наименование разделов и тем	Всего часов	Аудиторные за- нятия			Сам. Раб.
			ЛК	ПЗ	ЛБ	
7 семестр						
Раздел 1. Основные типы аудита информационной безопасности		22	3	3	6	10
1	Тема 1. Основные возможности современных методик анализа рисков и аудита ИБ.	8	1	1	2	4
2	Тема 2. Цели проведения АИБ. Базовые угрозы ИБ, учитываемые при проведении аудита. Особенности проведения внешнего и внутреннего аудита.	6	1	1	2	2
3	Тема 3. Основные типы аудита ИБ с учетом охвата им объектов защиты. Особенности сетевого аудита.	8	1	1	2	4
Раздел 2. Базовые этапы аудита информационной безопасности		28	4	4	8	12
4	Тема 4. Организационные вопросы, решение которых целесообразно на этапе инициирования процедуры аудита. Базовая документация, необходимая аудиторской группе для выполнения аудита.	8	1	1	2	4
5	Тема 5. Основные подходы, используемые аудиторами при анализе данных аудита	6	1	1	2	2
6	Тема 6. Особенности рекомендаций аудиторской группы по итогам аудита.	8	1	1	2	4
7	Тема 7. Структура и содержание основных разделов аудиторского отчёта.	6	1	1	2	2
Раздел 3. Основные направления аудита информационной безопасности		22	3	3	6	10
8	Тема 8. Основные составляющие аттестации объектов информатизации. Базовые компоненты контроля защищенности информации ограниченного доступа.	8	1	1	2	4
9	Тема 9. Состав специальных исследований технических средств на наличие побочных электромагнитных излучений и наводок. Особенности	8	1	1	2	4

	проектирования объектов информатизации в защищенном исполнении.					
10	Тема 10. Основные виды АИБ. Базовые процедуры, реализуемые при проведении активного аудита.	6	1	1	2	2
	<i>Зачет</i>					
	<i>Контроль</i>					
	Итого за 7 семестр	72	10	10	20	32
	в т.ч. практическая подготовка	4		2	2	
8 семестр						
Раздел 4. Правовые аспекты аудита информационной безопасности и программные средства для его реализации		66	6	6	6	48
11	Тема 11. Международные стандарты и руководства в сфере АИБ	22	2	2	2	16
12	Тема 12. Структура стандарта BS7799. Особенности стандартов ISO 17799 и ISO 15408. Структура стандарта COBIT. Основные этапы проведения аудита в соответствии со стандартом COBIT. Особенности стандартов BSI/IT, SYSTRUST и GIAC.	22	2	2	2	16
13	Тема 13. Характеристика международных стандартов серии ISO/IEC 27000.	22	2	2	2	16
Раздел 5. Общая модель процесса аудита защищенности информационного объекта		44	4	4	4	32
14	Тема 14. Аудит информационной безопасности (организации, автоматизированной системы), аудита информационной безопасности.	22	2	2	2	16
15	Тема 15. Назначение, цель аудита информационной безопасности (ИБ) объекта.	22	2	2	2	16
Раздел 6. Этапы, процедуры аудита информационной безопасности защищённых автоматизированных систем и организаций		60,7	4	4	4	48,7
16	Тема 16. Взаимодействие аудиторской организации с проверяемой организацией.	22	2	2	2	16
17	Тема 17. Ответственность аудиторской организации и проверяемой организации.	19	1	1	1	16
18	Тема 18. Определение области аудита ИБ, критериев аудита ИБ.	19,7	1	1	1	16,7
	<i>Экзамен</i>	0,3				
	<i>Контроль</i>	9				
	Итого за 8 семестр	180	14	14	14	128,7
	в т.ч. практическая подготовка	4		2	2	
	ИТОГО	288	24	24	34	288

Очно-заочная форма обучения
(не реализуется)

Заочная форма обучения
(не реализуется)

**III. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И
ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ**

Текущая аттестация проводится в форме теста.

Типовой вариант теста

Вопрос №1. Информационная составляющая присутствует в следующей категории рисков

Варианты ответов:

1. коммерческом
2. политическом
3. транспортном
4. во всех вышеуказанных рисках

Вопрос №2. Какой подход к обеспечению безопасности имеет место:

Варианты ответов:

1. теоретический
2. комплексный
3. логический

Вопрос №3. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

Варианты ответов:

1. Анализ рисков
2. Анализ затрат / выгоды
3. Результаты ALE
4. Выявление уязвимостей и угроз, являющихся причиной риска

Вопрос №4. Что является определением воздействия (exposure) на безопасность?

Варианты ответов:

1. Нечто, приводящее к ущербу от угрозы
2. Любая потенциальная опасность для информации или систем
3. Любой недостаток или отсутствие информационной безопасности
4. Потенциальные потери от угрозы

Вопрос №5. Эффективная программа безопасности требует сбалансированного применения:

Варианты ответов:

1. Технических и не технических методов
2. Контрмер и защитных механизмов

3. Физической безопасности и технических средств защиты
4. Процедур безопасности и шифрования

Промежуточная аттестация обучающихся осуществляется в форме зачета, экзамена с использованием следующих оценочных материалов: *перечень вопросов к зачету, перечень вопросов к экзамену.*

**Вопросы к зачету
(7 семестр, очная форма обучения)**

1. Основные задачи государственной системы ИБ.
2. Понятия внешнего и внутреннего аудита ИБ.
3. Основные услуги аудита информационной безопасности.
4. Цели проведения аудита информационной безопасности.
5. Основные типы аудита ИБ.
6. Особенности сетевого аудита.
7. Основные этапы аудита.
8. Базовые факторы, способствующие повышению уязвимости информации.
9. Организационные вопросы, решаемые на этапе инициирования процедуры аудита.
10. Основные разделы отчета по результатам аудита безопасности ИС.
11. Базовые виды угроз информационной безопасности.
12. Рейтинг защищаемых ресурсов ИС.
13. Базовые задачи и этапы комплексного аудита ИБ систем.
14. Основные задачи государственной системы ИБ.
15. Понятия внешнего и внутреннего аудита ИБ.
16. Основные услуги аудита информационной безопасности.
17. Цели проведения аудита информационной безопасности.
18. Основные типы аудита ИБ.
19. Особенности сетевого аудита.
20. Основные этапы аудита.
21. Базовые факторы, способствующие повышению уязвимости информации.
22. Организационные вопросы, решаемые на этапе инициирования процедуры аудита.
23. Основные разделы отчета по результатам аудита безопасности ИС.
24. Базовые виды угроз информационной безопасности.
25. Рейтинг защищаемых ресурсов ИС.
26. Базовые задачи и этапы комплексного аудита ИБ систем.
27. Основные этапы аудита безопасности внешнего периметра сети

**Вопросы к экзамену
(8 семестр, очная форма обучения)**

1. Основные виды аудита.
2. Базовые результаты экспертного аудита.
3. Основные методы тестирования ИС.
4. Общая характеристика сетевого сканера NetRecon.

5. Основные компоненты стандарта COBIT.
6. Базовые этапы проведения аудита при использовании стандарта COBIT.
7. Общая характеристика сетевого сканера XSpider.
8. Структура стандарта BS7799.
9. Анализ уровня защищённости интернет-сайтов с помощью GIAC.
10. Структура немецкого стандарта BSI/IT.
11. Общая характеристика семейства международных стандартов ISO/IEC 27000.
12. Необходимость аудита ИБ. 40. Виды аудита ИБ.
13. Критерии аудита ИБ.
14. Принципы аудита ИБ.
15. Роли при проведении аудита ИБ.
16. Сбор свидетельств аудита ИБ.
17. Анализ свидетельств аудита ИБ.
18. Завершение аудита ИБ.
19. Отчёт и заключение по результатам аудита ИБ.
20. Оценка соответствия ИБ автоматизированных организаций требованиям нормативных документов по ИБ.
21. Процессноориентированная оценка ИБ объекта.
22. Рискоориентированная оценка ИБ объекта.

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Основная литература

1. Информационные технологии в менеджменте (управлении) : учебник и практикум для вузов / Ю. Д. Романова [и др.] ; под редакцией Ю. Д. Романовой. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 467 с. — (Высшее образование). — ISBN 978-5-534-17037-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/532217> (дата обращения: 01.09.2023).

4.2. Дополнительная литература

1. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/531084> (дата обращения: 01.09.2023).

V. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫХ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

№ пп	Ссылка на информационный ресурс	Наименование разработки в электронной форме	Доступность
---------	------------------------------------	--	-------------

1.	http://edu.ru/	Российское образование: Федеральный портал. Включает ссылки на порталы и сайты образовательных учреждений; государственные образовательные стандарты; нормативные документы; каталог экскурсий и обучающих программ.	Свободный доступ
2.	http://citforum.ru/database/osbd/contents.shtml	Информационно-аналитические материалы	Свободный доступ

VI. СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1.	http://www.biblioclub.ru	Электронно-библиотечная система (ЭБС) Университетская библиотека онлайн	Регистрация через любой университетский компьютер. В дальнейшем предоставляется неограниченный индивидуальный доступ из любой точки, в которой имеется доступ к сети Интернет
2.	www.garant.ru	Информационно-правовой портал	Свободный доступ
3.	www.elibrary.ru	Российский информационный портал в области науки, технологии, медицины и образования	Свободный доступ
4.	www.consultant.ru	Российская компьютерная справочно-правовая система	Свободный доступ

VII. ЛИЦЕНЗИОННОЕ И СВОБОДНО РАСПРОСТРАНЯЕМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

При реализации учебной дисциплины применяется следующее лицензионное и свободно распространяемое программное обеспечение:

- Microsoft Windows;
- Microsoft Office;
- Libre Office и др.

VIII. ОБОРУДОВАНИЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА ОБУЧЕНИЯ, НЕОБХОДИМЫЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Учебные занятия проводятся в аудиториях, укомплектованных специализированной мебелью, в том числе стационарными или переносными техническими средствами обучения (проектор, экран, компьютер/ноутбук).

Лабораторные занятия, групповые и индивидуальные консультации, текущая и промежуточная аттестации проводятся в специализированных компьютерных классах. Перечень основного оборудования: автоматизированные рабочие места с компьютерами, программное обеспечение общего и профессионального назначения.

Самостоятельная работа проводится в кабинетах, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Предусмотрены помещения для хранения и профилактического обслуживания учебного оборудования.