ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. И.А. БУНИНА

«УТВЕРЖДАЮ»
Директор института математики, естествознания и техники
_____/Н.В.Черноусова/

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.О.04.13 Аудит защищенности информационного объекта

Направление подготовки: *10.03.01 Информационная безопасность*
Направленность (профиль): *Организация и технологии 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			
Форма(ы) промежуточной аттестации	**Зачет Экзамен - 0,3**		
Контроль	**9**		
Иные формы работы			
Самостоятельная работа	**196,7**		

Всего часов: 288
Трудоемкость: 8 зачетных единицы.
Разработчик(и) рабочей программы:
кандидат физико-математических наук, доцент С.А. Рощупкин

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины:

изучение обучающимися видов, практических методов и средств проведения аудита защищенности информационного объекта.

Задачи изучения дисциплины:

− формирование понимания процессов проверки и оценки защищенности информационного объекта, принципов организации процессов аудита и анализа рисков защищенности информационного объекта и подготовки отчетных документов;

− ознакомление с основными стандартами в области аудита защищенности информационного объекта, практическими приемами проведения аудита, методами сбора данных, оценки рисков и анализа защищенности;

− обучение инструментальным средствам проведения аудита защищенности информационного объекта.

Место дисциплины в структуре ОПОП: реализуется в рамках базовой части блока Б1. Дисциплины (модули).

Планируемые результаты обучения по дисциплине:

Код компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-5	**Знать**: - основные нормативно-правовые акты и иные документы, регламентирующие деятельность по защите информации; - организационно-управленческие методы и инструментарий, обеспечивающие деятельность по защите информации в сфере профессиональной деятельности.	**Знает:** - теоретические основы построения и функционирования информационных систем аудита; - основные стандарты, регламентирующие управление качеством информационной безопасности; - организационно-правовую документацию предприятий (устав, положение о предприятии), работающих в сфере защиты информации.
	Уметь: - использовать нормативно-правовые документы, связанные с обеспечением профессиональной деятельности на объектах защиты; - обосновывать организационно-управленческие решения в области обеспечения информационной безопасности систем, подлежащих информационной защите.	**Умеет:** - применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности.
	Владеть: - навыками аналитической работы с нормативно-правовыми документами, в частности с нормативной базой РФ, в сфере профессиональной деятельности на конкретных объектах защиты;	**Владеет:** - навыками работы с нормативными правовыми актами; - методами обработки результатов анализа данных аудита и содержащие оценку уровней защищенности

	- методами разработки проектов нормативных и организационно-распорядительных документов для конкретных объектов защиты.	объекта информатизации или соответствие ее требованиям стандартов; - навыками определения наиболее вероятных угроз безопасности в отношении ресурсов ИС и уязвимостей защиты, делающих возможным осуществление этих угроз.
ОПК-12	**Знать**: - перечень необходимых исходных данных для проектирования подсистем и средств обеспечения защиты информации, основные возможные проектные решения автоматизированных систем и подсистем, средства их защиты; - правила выполнения технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности.	**Знает:** - основные методы и технологию управления службой защиты информации; - организацию аудита информационной безопасности информационной системы; - методологию оценки информационных рисков объектов информатизации.
	Уметь: - проводить анализ исходных данных для проектирования подсистем передачи информации и средств обеспечения информационной безопасности; - проводить технико-экономический анализ и обоснование проектных решений, связанных с обеспечением информационной безопасности.	**Умеет:** - применять отечественные и зарубежные стандарты для проектирования, разработки и оценки защищенности объектов.
	Владеть: - навыками обеспечения информационной безопасности исходных данных для проектирования подсистем и средств; - навыками выполнения технико-экономического анализа и обоснования проектных решений, связанных с обеспечением информационной безопасности.	**Владеет:** - методами организации и управления деятельностью служб защиты информации на предприятии; - методами формирования требований по защите информации.
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:** - порядок проведения категорирования технических средств и систем аттестации объектов информатизации (выделенных помещений) требованиям безопасности информации.
	Уметь: - осуществлять мероприятия комплексного аудита, оценивать	**Умеет:** - реализовывать системы защиты информации в соответствии со

	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.	стандартами по оценке защищенных систем.
	Владеть: - методами сбора и оценки соответствия свидетельств аудита информационной безопасности защищённых автоматизированных систем нормативным требованиям по защите информации; - навыками оформления отчетной документации по результатам аудита объекта защиты.	**Владеет:** - методами и средствами выявления угроз безопасности объекту информатизации; - методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов

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 занятия			Сам. Раб.
			ЛК	ПЗ	ЛБ	
7 семестр						
Раздел 1. «Аудит защищенности информационного объекта»		**108**	**10**	**10**	**20**	**68**
1	Тема 1. Аудит безопасности и методы его проведения. Понятие аудита безопасности. Методы анализа данных при аудите ИБ. Анализ информационных рисков предприятия. Методы оценивания информационных рисков.	30	2	2	6	20
2	Тема 2. Оценка безопасности на основе «Общих критериев». Основные понятия ОК. Методология оценки безопасности информационных технологий по ОК. Оценка уровня доверия функциональной безопасности информационной технологии. Обзор классов и семейств ОК. Программные средства для проведения аудита ИБ. Анализ видов используемых программных продуктов. Система CRAMM. Система КОНДОР. Сетевые сканеры.	40	4	4	8	24
3	Тема 3. Методика проведения аудита информационной безопасности на предприятии. Задачи и содержание работ при проведении аудита ИБ. Подготовка предприятия к проведению аудита ИБ. Планирование процедуры	38	4	4	6	24

	аудита ИБ. Организация и проведение работ по аудиту. Алгоритм проведения аудита безопасности предприятия. Перечень и систематизация данных, необходимых для проведения аудита ИБ. Выработка рекомендаций и подготовка отчетных документов. Экономическая оценка обеспечения ИБ.					
	Форма отчетности	зачет				
	Зачет					
	Итого за 7 семестр	***108***	***10***	***10***	***20***	***68***
	в т.ч. практическая подготовка					
	8 семестр					
Раздел 2. «Анализ рисков ИБ»		**66**	**10**	**6**	**10**	**40**
4	Тема 4. Анализ рисков в области защиты информации. Информационная безопасность бизнеса. Развитие службы информационной безопасности. Международная практика защиты информации.	16	2	2	2	10
5	Тема 5. Модель Symantec LifeCycle Security. Постановка задачи анализа рисков. Модель Gartner Group. Модель Carnegie Mellon University. Различные взгляды на защиту информации.	17	4	1	2	10
6	Тема 6. Национальные особенности защиты информации. Особенности отечественных нормативных документов. Учет остаточных рисков.	17	2	1	4	10
7	Тема 7. Управление рисками и международные стандарты. Международный стандарт ISO 17799. Обзор стандарта BS 7799. Развитие стандарта BS 7799 (ISO 17799). Сравнение стандартов ISO 17799 и BSI. Стандарт США NIST 800-30. Алгоритм описания информационной системы. Идентификация угроз и уязвимостей. Организация защиты информации. Ведомственные и корпоративные стандарты управления ИБ. XBSS-спецификации сервисов безопасности X/Open. Стандарт NASA «Безопасность информационных технологий». Концепция управления рисками MITRE.	16	2	2	2	10
Раздел 3. «Технологии анализа рисков»		**68,7**	**10**	**4**	**10**	**44,7**
8	Тема 8. Вопросы анализа рисков и управления ими. Идентификация рисков. Оценивание рисков. Измерение рисков. Выбор допустимого уровня риска. Выбор контрмер и оценка их эффективности. Разработка корпоративной методики анализа рисков.	21	2	1	2	16
9	Тема 9. Постановка задачи. Методы оценивания информационных рисков. Табличные методы оценки рисков. Методика анализа рисков.	25	4	1	4	16
10	Тема 10. Инструментарий базового уровня. Справочные и методические материалы. COBRA. RA Software Tool. Средства полного	22,7	4	2	4	12,7

	анализа рисков. Метод CRAMM. Пример использования метода CRAMM. Средства компании MethodWare. Экспертная система «Аван-Гард». RiskWatch.					
	Форма отчетности	*экзамен*				
	Контроль	**9**				
	Экзамен	**0,3**				
	Итого за 8 семестр	***180***	***14***	***14***	***14***	***128,7***
	в т.ч. практическая подготовка					
	ИТОГО	**288**	**24**	**24**	**34**	**196,7**

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 контрольной работы.

Типовой вариант контрольной работы

1. Понятие аудита безопасности
2. Методы анализа данных при аудите ИБ
3. Анализ информационных рисков предприятия
4. Методы оценивания информационных рисков
5. Стандарт «Критерии оценки надежности компьютерных систем» (Оранжевая книга)
6. Гармонизированные критерии Европейских стран
7. Германский стандарт BSI
8. Британский стандарт BS 7799
9. Международный стандарт ISO 17799
10. Международный стандарт ISO 15408 «Общие критерии»
11. Стандарт COBIT
12. Стандарты по безопасности информационных технологий в России

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

Вопросы к зачету
(7 семестр, очная форма обучения)

1. Основные понятия общих критериев (ОК).
2. Методология оценки безопасности информационных технологий по ОК.

3. Оценка уровня доверия функциональной безопасности информационной технологии.

4. Обзор классов и семейств ОК.

5. Назначение стандарта ISO 17799 для управления информационной безопасностью.

6. Практика прохождения аудита и получения сертификата ISO 17799.

7. Анализ видов используемых программных продуктов.

8. Система CRAMM.

9. Система КОНДОР.

10. Сетевые сканеры.

11. Задачи и содержание работ при проведении аудита ИБ.

12. Подготовка предприятия к проведению аудита ИБ.

13. Планирование процедуры аудита ИБ.

14. Организация и проведение работ по аудиту.

15. Алгоритм проведения аудита безопасности предприятия.

16. Перечень и систематизация данных, необходимых для проведения аудита ИБ.

17. Выработка рекомендаций и подготовка отчетных документов.

18. Экономическая оценка обеспечения ИБ.

Вопросы к экзамену
(8 семестр, очная форма обучения)

1. Информационная безопасность бизнеса.
2. Развитие службы информационной безопасности.
3. Международная практика защиты информации.
4. Модель Symantec LifeCycle Security.
5. Постановка задачи анализа рисков.
6. Модель Gartner Group.
7. Модель Carnegie Mellon University.
8. Различные взгляды на защиту информации.
9. Национальные особенности защиты информации.
10. Особенности отечественных нормативных документов.
11. Учет остаточных рисков.
12. Международный стандарт ISO 17799.
13. Обзор стандарта BS 7799.
14. Развитие стандарта BS 7799 (ISO 17799).
15. Сравнение стандартов ISO 17799 и BSI.
16. Стандарт США NIST 800-30.
17. Алгоритм описания информационной системы.
18. Идентификация угроз и уязвимостей. Организация защиты информации.
19. Ведомственные и корпоративные стандарты управления ИБ.
20. XBSS-спецификации сервисов безопасности X/Open.
21. Стандарт NASA «Безопасность информационных технологий».
22. Концепция управления рисками MITRE.

23. Вопросы анализа рисков и управления ими.
24. Идентификация рисков.
25. Оценивание рисков.
26. Измерение рисков.
27. Выбор допустимого уровня риска.
28. Выбор контрмер и оценка их эффективности.
29. Разработка корпоративной методики анализа рисков.
30. Постановка задачи.
31. Методы оценивания информационных рисков.
32. Табличные методы оценки рисков.
33. Методика анализа рисков.

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Основная литература

1. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2021. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519780 (дата обращения: 01.09.2021).

4.2. Дополнительная литература

1. Нетесова, О. Ю. Информационные системы и технологии в экономике : учебное пособие для вузов / О. Ю. Нетесова. — 3-е изд., испр. и доп. — Москва : Издательство Юрайт, 2021. — 178 с. — (Высшее образование). — ISBN 978-5-534-08223-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491479 (дата обращения: 01.09.2021).

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; норма-	Свободный доступ

		тивные документы; каталог экскурсий и обучающих программ.	
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 компьютер-

ных 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.