ЕЛЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. И.А. БУНИНА

«УТВЕРЖДАЮ»
Директор института цифровых технологий и математики
_____ С.А. Рощупкин

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.01.14 Аттестация объектов информатизации

Направление подготовки: 10.03.01 Информационная безопасность
Направленность (профиль): Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)
Квалификация (степень): *бакалавр*
Форма обучения: *очная*

Институт: цифровых технологий и математики
Кафедра: математического моделирования, компьютерных технологий и информационной безопасности

	очная форма	**очно-заочная форма**	**заочная форма**
Курс	**4**		
Семестр	**8**		

Лекции	**8**		
Лабораторные занятия	**16**		
Практические (семинарские) занятия	**8**		
в т. ч. практическая подготовка	**6**		
Форма(ы) промежуточной аттестации	**Зачет**		
Контроль			
Иные формы работы			
Самостоятельная работа	**40**		

Всего часов: 72
Трудоемкость: 2 **зачетных единицы.**
Разработчик(и) рабочей программы: *кандидат педагогических наук, доцент* Л.Н. Александрова

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Цель изучения дисциплины:

формирование у обучающихся знаний, умений и навыков по вопросам аттестационных испытаний и аттестации на соответствие требованиям по защите информации.

Задачи изучения дисциплины:

- организация аттестации автоматизированных систем по требованиям безопасности информации;
- анализ исходных данных и документации по защите информации и проверка их соответствия реальным условиям размещения и эксплуатации автоматизированных систем;
- разработка программы и методик аттестационных испытаний;
- контроль соответствия системы защиты информации требованиям безопасности в процессе ее эксплуатации.

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
ПКС-1	**Знать:** - сущность и понятие информационной безопасности, характеристику ее составляющих, источники угроз и меры по их предотвращению; - методы и средства управления информационной безопасностью, а также основные подходы к разработке, реализации, эксплуатации, диагностике, анализу, сопровождению и совершенствованию систем защиты информации.	**Знает:** - основные угрозы информационной безопасности объекта информатизации и их классификацию; - классификацию мероприятий по защите информации, порядок проведения аттестации объектов информационной защиты; - типовые методики испытаний объектов информатизации по требованиям защиты информации; - типовые формы документов по подготовке и проведению сертификации и аттестации объектов защиты информации.
	Уметь: - оценивать защищенность, классифицировать основные угрозы, обеспечивать информационную безопасность компьютерных систем, применяя необходимые программно-аппаратные средства и системы защиты информации; - принимать управленческие и административные решения в сфере защиты информации.	**Умеет**: - определять угрозы объекту информатизации; - определять рациональные способы и средства защиты информации на объекте информатизации; - организовывать мероприятия по защите информации на объекте информатизации.
	Владеть: - категориальным аппаратом в области обеспечения комплекса мер	**Владеет:** - методами работы с действующей нормативно-правовой и

	по администрированию и диагностике систем защиты информации; - правилами, методами, средствами, процедурами управления и администрирования информационной безопасностью объекта.	методической базой в области технической защиты информации; - способами проведения аттестационных испытаний и аттестаций объектов информатизации на соответствие требованиям по защите информации; - методами оформления материалов аттестационных испытаний.

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	
Раздел 1. Основные принципы, организационная структура системы аттестации объектов информатизации по требованиям безопасности информации		**18**	**2**	**2**	**4**	**10**
1	Тема 1. Орган по аттестации. Порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации	9	1	1	2	5
2	Тема 2. Правовой статус аттестата соответствия	9	1	1	2	5
Раздел 2. Методические указания о порядке аттестации объектов информатизации		**22**	**3**	**3**	**4**	**12**
3	Тема 3. Методические указания о порядке аттестации объектов информатизации по требованиям безопасности	12	2	2	2	6
4	Тема 4. Методические рекомендации по организации и проведению работ по обеспечению безопасности информации в информационных системах персональных данных	10	1	1	2	6
Раздел 3. Документация, сопровождающая аттестационные испытания		**32**	**3**	**3**	**8**	**18**
5	Тема 5. Эксплуатация аттестованных объектов информатизации	12	1	1	4	6
6	Тема 6. Классификация специальных защитных знаков	10	1	1	2	6
7	Тема 7. Документация, сопровождающая аттестационные испытания	10	1	1	2	6
	Зачет					
	Контроль					
	Итого за 8 семестр	***72***	***8***	***8***	***16***	***40***

	в т.ч. практическая подготовка	***6***		***2***	***2***	***2***
	ИТОГО	***72***	***8***	***8***	***16***	***40***

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 в виде теста.

1. Определите процедуру, которая должна быть проведена с целью оценки соответствия требованиям по безопасности информации принятых на объекте мер по защите информации:
   а) Сертификация
   б) Аттестация
   в) Аккредитация
   г) Лицензирование
2. Выберите виды информации при классификации ее по категориям доступа:
   а) Открытая информация
   б) Общедоступная информация
   в) Информация ограниченного доступа
   г) Секретная информация
   д) Информация свободного доступа
   е) Конфиденциальная информация
   ж) Свободно распространяемая информация
3. Информация какого вида, в соответствие с федеральными законами, не может быть отнесена к информации ограниченного доступа:
   а) Государственная тайна
   б) Информация о состоянии окружающей среды
   в) Информация о частной жизни гражданина
   г) Тайна голосования
   д) Нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина
   е) Тайна переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений
4. Какая информация не относится к сведениям конфиденциального характера, исходя из «Перечня сведений конфиденциального характера», утвержденным Указом Президента РФ от 6 марта 1997 г. N 188:
   а) Персональные данные
   б) Государственная тайна
   в) Тайна следствия и судопроизводства
   г) Общедоступная информация
   д) Служебная тайна
   е) Информация ограниченного доступа
5. Выберите объект испытаний при проведении процедуры аттестации:
   а) Индивидуальный предприниматель
   б) Средство контроля эффективности защиты информации

в) Помещение для проведения конфиденциальных переговоров
г) Юридическое лицо

6. Выберите из ниже предложенного объекты информатизации, подлежащие защите:
а) Автоматизированные системы
б) Средство защиты информации
в) Система размножения документов
г) Средство контроля эффективности защиты информации

7. Выберите объект испытаний при проведении процедуры лицензирования:
а) Объект информатизации
б) Средство защиты информации
в) Автоматизированная система
г) Юридическое лицо

8. Выберите из ниже предложенного организационные мероприятия (возможно несколько вариантов):
а) Классификация автоматизированных систем
б) Установка шумоизолирующих прокладок на дверь
в) Составление перечня информации, подлежащей защите
г) Установка сертифицированной по требованиям безопасности информации операционной системы

9. Выберите объект испытаний при проведении процедуры сертификации:
а) Объект информатизации
б) Изделие
в) Помещение для ведения конфиденциальных переговоров
г) Индивидуальный предприниматель

10. В какой процедуре участвует третья сторона – испытательная лаборатория?
а) Аттестация
б) Аккредитация
в) Лицензирование
г) Сертификация

11. Специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности это:
а) Аттестат аккредитации
б) Сертификат соответствия
в) Лицензия
г) Аттестат соответствия
д) Заключение
е) Предписание

12. По результатам проведения комплекса организационно-технических мероприятий, в результате которых подтверждается, что объект информатизации соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации выдается:
а) Аттестат аккредитации
б) Сертификат соответствия
в) Лицензия
г) Заключение
д) Предписание
е) Аттестат соответствия

13. Какие меры защиты информации предусматривают использование конструктивных решений и технологических особенностей обработки информации ограниченного доступа на объектах информатизации?
а) Активные
б) Пассивные

в) Организационные пассивные
г) Организационные активные
д) Технические пассивные
е) Технические активные

14. При необходимости подтверждения соответствия системы активной защиты информации установленным требованиям проводится процедура:
а) Аттестации
б) Лицензирования
в) Сертификации
г) Аккредитации

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

Вопросы к зачету
(8 семестр, очная форма обучения)

1. Организационная структура системы аттестации объектов информатизации (ОИ) и их функции. Какие ОИ подлежат обязательной аттестации?
2. Федеральные органы по аттестации и их функции.
3. Органы по аттестации объектов и их функции. Задачи и функции органа по аттестации.
4. Деятельность аттестационных комиссий.
5. Права, обязанности и ответственность органов по проведению аттестации.
6. Аккредитация испытательных лабораторий и органов по сертификации средств защиты информации по требованию безопасности информации. Порядок аккредитации.
7. Контроль и надзор за деятельностью аккредитованных испытательных лабораторий и органов по сертификации.
8. Заявители и их функции. Заявка на проведение аттестации ОИ.
9. Порядок проведения аттестации объектов информатизации. Содержание заявок.
10. Порядок взаимодействия заявителя и органа по проведению аттестации.
11. Испытательные центры сертификации продукции по требованию безопасности, их функции.
12. Исходные данные и документация, представляемая заявителем для проведения аттестации.
13. Составляющие аттестационных испытаний объектов информатизации. Программа аттестации на объектах.
14. Проведение аттестации объектов информатизации. Этапы аттестации.
15. Порядок проведения аттестационных испытаний АС. Основные составляющие.
16. Порядок проведения аттестационных испытаний. Основные составляющие.
17. Заключительный этап аттестации ОИ. Условия получения аттестата соответствия.
18. Содержание заключения аттестационной комиссии.
19. Оформление, регистрация и выдача "Аттестата соответствия".
20. Эксплуатация аттестованного объекта.
21. Рассмотрение апелляций по вопросам аттестации.
22. Аттестационные испытания АС. Что входит в изучение технологического процесса обработки, передачи и хранения информации?
23. Аттестационные испытания АС. Что входит в изучение соответствия организационно-техническим требованиям по ЗИ?
24. Аттестационные испытания АС. Что входит в проверку требований по ЗИ от утечки по цепям заземления и питания.
25. Аттестационные испытания АС. Что входит в испытания на соответствие требованиям по ЗИ от несанкционированного доступа (НСД)?

26. Аттестационные испытания выделенного помещения (ВП). Что входит в проверку требований по ЗИ от утечки за счет ПЭМИН.
27. Аттестационные испытания выделенного помещения (ВП). Что входит в проверку систем ЗИ?
28. Аттестационные испытания ВП. Что входит в проверку систем ВТСС на отсутствие акустоэлектрических преобразований?

IV. ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

4.1. Основная литература

1. Аудит информационной безопасности органов исполнительной власти : учебное пособие : [16+] / В. И. Аверченков, М. Ю. Рытов, А. В. Кувыклин, М. В. Рудановский. – 5-е изд., стер. – Москва : ФЛИНТА, 2021. – 100 с. : ил., схем., табл. – (Организация и технология защиты информации). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93259 (дата обращения: 18.04.2025). – Библиогр.: с. 83-84. – ISBN 978-5-9765-1277-1. – Текст : электронный.

2. Данилова, О. Т. Технические средства разведки и защита информации : учебное пособие : в 4 частях : [16+] / О. Т. Данилова ; Омский государственный технический университет. – Омск : Омский государственный технический университет (ОмГТУ), 2019. – Часть 1. Технические каналы утечки речевой акустической конфиденциальной информации. – 64 с. : ил., табл., схем., граф. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=682094 (дата обращения: 18.04.2025). – Библиогр. в кн. – ISBN 978-5-8149-2839-9 (Ч. 1). - ISBN 978-5-8149-2838-2. – Текст : электронный.

4.2. Дополнительная литература

1. Аверченков, В. И. Служба защиты информации : организация и управление : учебное пособие : [16+] / В. И. Аверченков, М. Ю. Рытов. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 186 с. : ил., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93356 (дата обращения: 18.04.2025). – Библиогр. в кн. – ISBN 978-5-9765-1271-9. – Текст : электронный.

2. Организация безопасной работы информационных систем : учебное пособие / Ю. Ю. Громов, Ю. Ф. Мартемьянов, Ю. К. Букурако [и др.] ; Тамбовский государственный технический университет. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2014. – 132 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=277794 (дата обращения: 18.04.2025). – Библиогр. в кн. – Текст : электронный.

3. Попов, М. И. Разработка типовых документов для подготовки и оформления исходных данных по аттестации защищаемого помещения : выпускная квалификационная работа бакалавра / М. И. Попов ; Алтайский государственный технический университет им. И. И. Ползунова, Факультет информационных технологий, Кафедра Информатики, вычислительной техники и информационной безопасности. – Барнаул : , 2015. – 92 с. : табл., ил., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=490678 (дата обращения: 18.04.2025). – Текст : электронный.

4. Скрипник, Д. А. Общие вопросы технической защиты информации : учебное пособие / Д. А. Скрипник. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 425 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=429070 (дата обращения: 18.04.2025). – Библиогр. в кн. – Текст : электронный.

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.