МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра информационной безопасности

ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.03.01 Информационная безопасность
Код и наименование направления подготовки/специальности

«Организация и технология защиты информации
(по отрасли или в сфере профессиональной деятельности)»
Наименование направленности (профиля)/ специализации

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2023

ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ
Рабочая программа дисциплины

Составитель:
д.т.н, профессор В.В. Арутюнов

Ответственный редактор
к.и.н., доцент, заведующая кафедрой ИБ Г.А. Шевцова

УТВЕРЖДЕНО
Протокол заседания кафедры
Информационной безопасности
№ 9 от 17.03.2023

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

. Цель дисциплины: формирование навыков организации проведения комплекса организационно-технических мероприятий (аттестационных испытаний), в результате которых устанавливается соответствие защищаемого объекта требованиям стандартов и нормативно-технических документов по безопасности информации, утвержденных правовыми регуляторами РФ.

Задачи дисциплины: анализ функций органов аттестации, испытательных центров, заявителей и их взаимодействие при проведении аттестации объектов информатизации; изучение порядка проведения аттестации (разработка заявки на проведение аттестации, программы и методики аттестационных испытаний, их проведение), оформления и регистрации аттестата соответствия.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
ПК-5 Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	ПК-5.1 Знает нормативные правовые акты, методические документы, национальные стандарты в области защиты информации ограниченного доступа и аттестации объектов информатизации на соответствие требованиям по защите информации	Знать: базовые международные и российские регуляторы по информационной безопасности
	ПК-5.2 Умеет разрабатывать программы и методики аттестационных испытаний выделенных (защищаемых) помещений на соответствие требованиям по защите информации, проводить аттестационные испытания, оформлять заключение по результатам аттестации выделенных (защищаемых) помещений на соответствие требованиям по защите информации	Уметь: работать со стандартами и нормативными документами
	ПК-5.3 Владеет навыками подготовки аттестата соответствия выделенных (защищаемых) помещений требованиям по защите информации	Владеть: навыками использования международных и национальных стандартов в своей профессиональной деятельности
ПК-10 Способен проводить анализ информационной безопасности объектов и систем на соот-	ПК-10.1 Знает нормативные правовые акты в области защиты информации, национальные, межгосударственные и международ-	Знать: нормативные правовые акты в области защиты ПДн, национальные, межгосударственные и международные

ветствие требованиям стандартов в области информационной безопасности	ные стандарты в области защиты информации, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации	стандарты в области защиты ПДн; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите ПДн;
	ПК-10.2 Умеет анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки информации ограниченного доступа, установленных на объектах информатизации, и характере обрабатываемой на них информации	Уметь: анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки ПДн, установленных на объектах информатизации
	ПК-10.3 Владеет навыком разработки аналитического обоснования необходимости создания системы защиты информации в организации	Владеть: навыком разработки аналитического обоснования необходимости создания системы защиты ПДн в организации
ПК-15 Способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ПК-15.1 Знает технологический процесс защиты информации и процедуру разработки технических заданий, планов и графиков проведения работ по защите информации в соответствии с действующим нормативными и методическими документами	Знать: особенности практической деятельности организации и специфика защиты объекта
	ПК-15.2 Умеет применять национальные, межгосударственные и международные стандарты в области защиты информации, применять действующую законодательную базу в области обеспечения защиты информации, читать и понимать нормативные и методические документы по информационной безопасности на английском языке	Уметь: осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм
	ПК-15.3 Владеет навыками по контролю над соблюдением установленного порядка выполнения работ, а также действующего законодательства Российской Федерации при решении вопросов, касающихся защиты информации	Владеть: способностью Организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными и методическими документами ФСТЭК и ФСБ

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Организационное обеспечение аттестации объектов информатизации» относится к части, формируемой участниками образовательных отношений, блока дисциплин учебного плана. Для освоения дисциплины необходимы компетенции, сформированные в ходе изучения следующих дисциплины и прохождения практики: Методы принятия организационно-технических решений, Защита информации от несанкционированного доступа, Экономика защиты информации. В результате освоения дисциплины формируются компетенции, необходимые для изучения следующих дисциплин и прохождения практики: Аудит информационной безопасности, Системы информационно-аналитического мониторинга.

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет _3 з.е., 108 академических часа.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
5	Лекции	**26**
5	Практические работы	**28**
Всего:		**54**

Объем дисциплины в форме самостоятельной работы обучающихся составляет _54_ академических часа.

3. Содержание дисциплины

Тема 1. Назначение и общая характеристика аттестации и сертификации в области защиты информации

Предмет и содержание дисциплины, методы изучения, основная литература, контроль освоения дисциплины. Основные цели механизмов лицензирования и сертификации в России. Базовый нормативный документ в области сертификации и аттестации в России.

Цели и принципы сертификации. Понятие декларации о соответствии и обязательной сертификации. Содержание декларации о соответствии.

Сущность и состав сертификата соответствия. Основные схемы декларирования соответствия продукции. Основные принципы проведении сертификационных испытаний средств защиты информации. Сертификация продукции на международном уровне.

Тема 2. Основные требования к защищённости базовых объектов информатизации

Основная цель аттестации объектов информатизации. Базовые нормативные правовые акты в сфере сертификации и аттестации. Основные схемы аттестации объектов информатизации.

Аттестация автоматизированных систем и средств вычислительной техники (СВТ) в России в соответствии с руководящими документами (РД) ФСТЭК России. Перечень требований к защищенности автоматизированных систем в зависимости от класса защищенности. Перечень требований к защищенности СВТ в зависимости от класса защищенности.

Классификация программного обеспечения средств защиты информации по уровню

контроля отсутствия недекларированных возможностей. Классификация межсетевых экранов по уровню защищённости от НСД.

Тема 3. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации

Основные элементы системы аттестации объектов информатизации по требованиям безопасности информации. Структура органов по аттестации объектов информатизации, которые аккредитуются ФСТЭК России. Основные функции федерального органа по сертификации и аттестации. Базовые функции органов по аттестации объектов информатизации.

Основные работы испытательных центров (лабораторий) по сертификации продукции. Базовые виды работ заявителей аттестуемых объектов информатизации.

Тема 4. Порядок проведения аттестации объектов информатизации

Основные этапы проведения аттестации объектов информатизации. Содержание, порядок государственного контроля и надзора по аттестации объектов информатизации.

Содержание заявки заявителя для получения «Аттестата соответствия». Порядок проведения аттестационных испытаний. Исходные данные и документация, представляемая заявителем органу по аттестации.

Основные работы при проведении специального обследования аттестуемого объекта. Базовые работы, проводимые при аттестации объектов информатизации для каждого технического средства обработки информации (ТСОИ). Основные работы при аттестации выделенного помещения.

Структура заключения аттестационной проверки объекта информатизации. Содержание протокола аттестационных испытаний. Структура «Аттестата соответствия» объекта информатизации (выделенного помещения) требованиям по безопасности информации. Сущность контроля состояния защиты информации с целью своевременного выявления и предотвращения утечки информации по техническим каналам на предприятии. Категорирование объектов и определение режимных зон внутри них.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебной работы	Информационные и образовательные технологии
1.	Назначение и общая характеристика аттестации и сертификации в области защиты информации	Лекция 1 Практическая работа 1	Вводная лекция с использованием видеоматериалов опрос
2.	Основные требования к защищённости базовых объектов информатизации	Лекция 2 Практическая работа 2	Лекция с использованием видеопроектора опрос
3.	Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации	Лекция 3 Практическая работа 3	Лекция с использованием видеопроектора опрос

4.	Порядок проведения аттестации объектов информатизации	Лекция 4 Практическая работа 4 Контрольная работа	Лекция с использованием видеопроектора Опрос Подготовка к контрольной с использованием материалов лекций и литературы

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:

– видео-лекции**;**

– онлайн-лекции в режиме реального времени;

– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;

– системы для электронного тестирования;

– консультации с использованием телекоммуникационных средств.

5. Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: - *опрос* - *контрольная работа (темы 3-4)*	 *10 баллов* *20 баллов*	 *40 баллов* *20 баллов*
Промежуточная аттестация – зачет без оценки (вопросы по билетам)		*40 баллов*
Итого за семестр		*100 баллов*

5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	зачтено	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
82-68/ C	зачтено	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	зачтено	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Устный опрос

Устный опрос – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объёма знаний, обучающегося по определённому разделу, теме, проблеме и т.п.

Примерная тематика вопросов для опроса:

Вопросы	*Реализуемая компетенция*
1. Базовые органы - генераторы правовых документов в сфере ИБ в России на федеральном уровне	***ПК-5***
2. Объекты информатизации, аттестуемые по требованиям безопасности информации.	***ПК-15***
3. Основные виды работ, проводимые в соответствии со схемой аттестации.	***ПК-15***
4. Базовые категории аттестуемых объектов информатизации	***ПК-10***

Примерная тематика контрольной работы - проверка сформированности компетенций ПК-5, ПК-10,ПК-15

1. Содержание декларации о соответствии.
2. Особенности различных схем декларирования соответствия продукции.
3. Содержание сертификата соответствия.
4. Сведения, содержащиеся в сертификате на продукцию.
5. Базовые уровни сертификации для систем конфиденциального электронного документооборота.
6. Основные виды документов, используемые при проведении сертификационных испытаний. .
7. Базовые разделы методики сертификационных испытаний.
8. Содержание протокола сертификационных испытаний.
9. Основные группы классификация автоматизированных систем в соответствии с требованиями по защите информации.
10. Базовые группы показателей защищённости СВТ.
11. Основные группы требований к защищенности АС в зависимости от класса их защищенности.
12. Классификация МЭ по уровню контроля отсутствия незадекларированных возможностей.
13. Функции органов по аттестации объектов информатизации.
14. Состав программы аттестационных испытаний.
15. Базовые действия при аттестации выделенного помещения.
16. Основные разделы протокола аттестационных испытаний.

Промежуточная аттестация (примерные контрольные вопросы по курсу) - проверка сформированности компетенций ПК-5, ПК-10,ПК-15

1. Основные цели сертификации в России в области защиты информации.
2. Характеристика базовых органов - генераторов правовых документов в сфере ИБ в России на федеральном уровне.
3. Основные принципы, обеспечивающие эффективность сертификации.
4. Содержание декларации о соответствии.
5. Особенности различных схем декларирования соответствия продукции.
6. Основные принципы проведении сертификационных испытаний средств защиты информации.
7. Основные разделы пользовательской документации для импортного ПО.
8. Базовые объекты информатизации, аттестуемые в соответствии с требованиям безопасности информации.
9. Основные виды работ, проводимые в соответствии со схемой аттестации.
10. Перечень необходимых работ для выбора схемы аттестации.
11. Классификация автоматизированных систем в соответствии с требованиями по защите информации.
12. Классификация СВТ в соответствии с требованиями по защите информации.
13. Основные требования по защите, предъявляемые к межсетевым экранам.
14. Классификация программного обеспечения по уровню контроля отсутствия недекларированных возможностей.
15. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации.
16. Основные работы заявителей для проведения аттестации

объектов информатизации.
17. Базовые этапы проведения аттестации.
18. Содержание программы аттестационных испытаний.
19. Основные категории аттестуемых объектов информатизации.
20. Базовые зоны безопасности аттестуемых объектов информатизации.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Литература
Основная

1. *Олифер В.Г.* Компьютерные сети : принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. – 3-е изд. – М. [и др.] : Питер, 2008. – 957 с.
2. *Митюшин Д.А.* Использование программного комплекса CiscoPacketTracer v.7.3 в изучении сетевых технологий: учебно-практическое пособие (практикум) / Д. А. Митюшин ; Российский государственный гуманитарный университет. – М.: Изд-во РГГУ, 2021. – 217 с.
3. Голиков А. М. Основы проектирования защищенных телекоммуникационных систем: учебное пособие, Томск: ТУСУР, 2016. –396 с., http://biblioclub.ru
4. Поликанин, А. Н. Технические средства охраны и видеонаблюдения. Системы видеонаблюдения и тепловизионного контроля : учебное пособие / А. Н. Поликанин. — Новосибирск :СГУГиТ, 2021. — 46 с. — ISBN 978-5-907320-92-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/222380 (дата обращения: 01.04.2023). — Режим доступа: для авториз. пользователей.

Дополнительная

1. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/
2. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. http://rkn.gov.ru/Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.
2. Nginx.org – [Электронный ресурс] : Режим доступа : https://nginx.org/ru, свободный. – Загл. с экрана
3. WiresharkDeveloper’sGuide [Электронный ресурс]: Режим доступа: https://www.wireshark.org/docs/wsdg_html_chunked/, свободный. – Загл. с экрана

Национальная электронная библиотека (НЭБ) www.rusneb.ru
ELibrary.ru Научная электронная библиотека www.elibrary.ru
Электронная библиотека Grebennikon.ruwww.grebennikon.ru

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс

2. Гарант

7. Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения:

1) для лекционных занятий - учебная аудитория, доска, компьютер или ноутбук, проектор (стационарный или переносной) для демонстрации учебных материалов.

Состав программного обеспечения:
1. Windows
2. MicrosoftOffice
3. KasperskyEndpointSecurity

Для проведения занятий лекционного типа предлагаются тематические иллюстрации в формате презентаций PowerPoint.

2) для практических занятий – компьютерный класс или лаборатория, доска, проектор (стационарный или переносной), компьютер или ноутбук для преподавателя, компьютеры для обучающихся.

Состав программного обеспечения:
1. Windows
2. MicrosoftOffice
3. Kaspersky Endpoint Security
4. Mozilla Firefox
5. Cisco Packet Tracer v.7.2

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализированным программным обеспечением или могут быть заменены устным ответом; обеспечивается индивидуальное равномерное освещение не менее 300 люкс; для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; письменные задания оформляются увеличенным шрифтом; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.
- для глухих и слабослышащих: лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования; письменные задания выполняются на компьютере в письменной форме; экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.
- для лиц с нарушениями опорно-двигательного аппарата: лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением; письменные задания выполняются на компьютере со специализиро-

ванным программным обеспечением; экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих: в печатной форме увеличенным шрифтом, в форме электронного документа, в форме аудиофайла.
- для глухих и слабослышащих: в печатной форме, в форме электронного документа.
- для обучающихся с нарушениями опорно-двигательного аппарата: в печатной форме, в форме электронного документа, в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих: устройством для сканирования и чтения с камерой SARA CE; дисплеем Брайля PAC Mate 20;принтером Брайля EmBrailleViewPlus;
- для глухих и слабослышащих: автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих; акустический усилитель и колонки;
- для обучающихся с нарушениями опорно-двигательного аппарата: передвижными, регулируемыми эргономическими партами СИ-1;компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1 Планы практических занятий

Темы учебной дисциплины предусматривают проведение практических занятий, которые служат как целям текущего и промежуточного контроля подготовки студентов, так и целям получения практических навыков применения методов выработки решений, закрепления изученного материала, развития умений, приобретения опыта решения конкретных проблем, ведения дискуссий, аргументации и защиты выбранного решения. Помощь в этом оказывают задания для практических занятий, выдаваемые преподавателем на каждом занятии.

Целью практических занятий является закрепление теоретического материала и приобретение практических навыков работы с соответствующим оборудованием, программным обеспечением и нормативными правовыми документами.

Тематика практических занятий соответствует программе дисциплины.

Практическое занятие 1. (Тема 1). Цели осуществления сертификации в России - (6 часов) - *проверка сформированности компетенций ПК-5, ПК-15*

Вопросы для изучения и обсуждения:

1. Базовые цели реализации сертификации в России.
2. Основные уровни сертификации для систем конфиденциального электронного документооборота.

3. Базовые органы - генераторы правовых документов в сфере ИБ в России на федеральном уровне.
4. Основные принципы, соблюдение которых необходимо при проведении сертификационных испытаний средств защиты информации.

Контрольные вопросы:

1. Понятие декларации о соответствии.
2. Основные документы, необходимые для регистрации системы добровольной сертификации.
3. Структура сертификата соответствия.
4. Содержание декларации о соответствии.

Список литературы:

Сапронова О. Аттестация объектов информатизации по требованиям безопасности информации [Электронный ресурс]. - Режим доступа: URL: https://www.intuit.ru/studies/courses/3648/890/info

Положение по аттестации объектов информатизации по требования безопасности информации. - М.: Гостехкомиссия РФ, 1994. - 22 с. - Режим доступа: URL:

https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g?highlight=

Макеев С.А. Содержание программы и методик проведения аттестационных испытаний информационных систем на соответствие требованиям безопасности информации // Правовая информатика. 2015. № 3. С. 19-23. - Режим доступа: URL: https://elibrary.ru/download/elibrary_27692421_57961861.pdf

Гавриленко А.Д. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации // Молодой ученый, № 5. - 2013. - С. 143-148. - Режим доступа: URL: https://moluch.ru/archive/52/

Информационный портал в области защиты информации - Режим доступа: http://www.securitylab.ru

Портал ФСТЭК России - Режим доступа: http://fstec.ru

Национальный открытый университет ИНТУИТ - Режим доступа: http://www.intuit.ru

Государственная публичная научно-техническая библиотека России - Режим доступа: http://www.gpntb.ru

Практическое занятие 2. (Тема 2). Аттестация автоматизированных систем, средств вычислительной техники и межсетевых экранов в России - (6 часов) - *проверка сформированности компетенций - ПК-10, ПК15*

Вопросы для изучения и обсуждения:

1. Основные схемы проведения аттестации объектов информатизации.
2. Базовые классы защищённости автоматизированных систем.
3. Основные группы защищённости СВТ.
4. Классификация программного обеспечения по уровню контроля отсутствия недекларированных возможностей.
5. Перечень требований защищенности СВТ.
6. Классификация межсетевых экранов по уровню защищённости от НСД.

Контрольные вопросы:

1. Понятие аттестации объектов информатизации.
2. Перечислите основные объекты информатизации, подлежащие аттестации.
3. В каких случаях аттестация носит обязательный или добровольный характер?
4. Перечислите нормативные правовые акты, определяющие основные принципы и организационную структуру системы аттестации и порядок проведения аттестации.
5. Основные требования по защите межсетевых экранов.
6. Перечислите основные подсистемы автоматизированных систем, для которых устанавливаются требования по их защищённости.

Список литературы:

Сапронова О. Аттестация объектов информатизации по требованиям безопасности информации [Электронный ресурс]. - Режим доступа: URL: https://www.intuit.ru/studies/courses/3648/890/info

Положение по аттестации объектов информатизации по требования безопасности информации. - М.: Гостехкомиссия РФ, 1994. - 22 с. - Режим доступа: URL:

https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g?highlight=

Макеев С.А. Содержание программы и методик проведения аттестационных испытаний информационных систем на соответствие требованиям безопасности информации // Правовая информатика. 2015. № 3. С. 19-23. - Режим доступа: URL: https://elibrary.ru/download/elibrary_27692421_57961861.pdf

Гавриленко А.Д. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации // Молодой ученый, № 5. - 2013. - С. 143-148. - Режим доступа: URL: https://moluch.ru/archive/52/

Портал ФСТЭК России - Режим доступа: http://fstec.ru

Национальный открытый университет ИНТУИТ - Режим доступа: http://www.intuit.ru

Практическое занятие 3. (Тема 3). Основные элементы системы аттестации объектов информатизации по требованиям безопасности информации - (8 часов) - *проверка сформированности компетенций - ПК-5, ПК-15*

Вопросы для изучения и обсуждения:

1. Структурный состав системы аттестации объектов информатизации по требованиям безопасности информации.
2. Основные элементы органов по аттестации объектов информатизации.
3. Базовые функции федерального органа по сертификации и аттестации.
4. Основные функции органов по аттестации объектов информатизации.

Контрольные вопросы:

1. Перечислите элементы системы аттестации объектов информатизации по требованиям безопасности информации.
2. Основные работы заявителей для проведения аттестации объектов информатизации.
3. Какую работу проводят испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации?
4. Основные разделы заявки заявителя на проведение аттестации.

Список литературы:

Сапронова О. Аттестация объектов информатизации по требованиям безопасности информации [Электронный ресурс]. - Режим доступа: URL: https://www.intuit.ru/studies/courses/3648/890/info

Положение по аттестации объектов информатизации по требования безопасности информации. - М.: Гостехкомиссия РФ, 1994. - 22 с. - Режим доступа: URL:
https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g?highlight=

Макеев С.А. Содержание программы и методик проведения аттестационных испытаний информационных систем на соответствие требованиям безопасности информации // Правовая информатика. 2015. № 3. С. 19-23. - Режим доступа: URL: https://elibrary.ru/download/elibrary_27692421_57961861.pdf

Гавриленко А.Д. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации // Молодой ученый, № 5. - 2013. - С. 143-148. - Режим доступа: URL: https://moluch.ru/archive/52/

Портал ФСТЭК России - Режим доступа: http://fstec.ru

Национальный открытый университет ИНТУИТ - Режим доступа: http://www.intuit.ru

Практическое занятие 4. (Тема 4). Основные этапы проведения аттестации объектов информатизации - (8 часов) - *проверка сформированности компетенций - ПК-10, ПК-15*

Вопросы для изучения и обсуждения:

1. Сведения, представляемые заявителем для проведения аттестационных испытаний.
2. Основные работы, проводимые при проведении специального обследования аттестуемого объекта.
3. Базовые работы, проводимые при аттестации выделенного помещения.
4. Содержание программы аттестационных испытаний.
5. Основные категории аттестуемых объектов информатизации.

Контрольные вопросы:

1. Перечислите этапы проведения аттестации объектов информатизации.
2. Что реализуется на начальном этапе проведения аттестации объектов информатизации?
3. Что включает этап проведения аттестационных испытаний объекта информатизации?
4. Основные разделы заявки заявителя на получение «Аттестата соответствия».
5. Содержание протокола аттестационных испытаний.

Список литературы:

Сапронова О. Аттестация объектов информатизации по требованиям безопасности информации [Электронный ресурс]. - Режим доступа: URL: https://www.intuit.ru/studies/courses/3648/890/info

Положение по аттестации объектов информатизации по требования безопасности информации. - М.: Гостехкомиссия РФ, 1994. - 22 с. - Режим доступа: URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g?highlight=

Макеев С.А. Содержание программы и методик проведения аттестационных испытаний информационных систем на соответствие требованиям безопасности информации // Правовая информатика. 2015. № 3. С. 19-23. - Режим доступа: URL: https://elibrary.ru/download/elibrary_27692421_57961861.pdf

Гавриленко А.Д. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации // Молодой ученый, № 5. - 2013. - С. 143-148. - Режим доступа: URL: https://moluch.ru/archive/52/

Портал ФСТЭК России - Режим доступа: http://fstec.ru

Национальный открытый университет ИНТУИТ - Режим доступа: http://www.intuit.ru

Приложение 1. Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Организационное обеспечение аттестации объектов информатизации» реализуется на факультете Информационных систем и безопасности кафедрой информационной безопасности.

Цель дисциплины: формирование навыков организации проведения комплекса организационно-технических мероприятий (аттестационных испытаний), в результате которых устанавливается соответствие защищаемого объекта требованиям стандартов и нормативно-технических документов по безопасности информации, утвержденных правовыми регуляторами РФ.

Задачи дисциплины: анализ функций органов аттестации, испытательных центров, заявителей и их взаимодействие при проведении аттестации объектов информатизации; изучение порядка проведения аттестации (разработка заявки на проведение аттестации, программы и методики аттестационных испытаний, их проведение), оформления и регистрации аттестата соответствия.

Дисциплина направлена на формирование следующих компетенций:

- ПК-5 – Способен принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
- ПК-10 – Способен проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности
- ПК-15 – Способен организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

В результате освоения дисциплины обучающийся должен:

- Знать: нормативные правовые акты в области защиты ПДн, национальные, межгосударственные и международные стандарты в области защиты ПДн; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите ПДн; особенности практической деятельности организации и специфика защиты объекта;

- Уметь: анализировать данные о назначении, функциях, условиях функционирования объектов и систем обработки ПДн, установленных на объектах информатизации; делать выводы по оценке защищённости ИСПДн на основании аналитического отчёта; осуществлять свою деятельность в различных сферах общественной жизни с учетом принятых в обществе моральных и правовых норм

- Владеть: навыками использования международных и национальных стандартов в своей профессиональной деятельности; способностью организовать технологический процесс защиты информации в соответствии с правовыми нормативными актами и нормативными и методическими документами ФСТЭК и ФСБ; навыком разработки аналитического обоснования необходимости создания системы защиты ПДн в организации;

По дисциплине предусмотрена промежуточная аттестация в форме зачета без оценки.
Общая трудоёмкость освоения дисциплины составляет 3 зачётные единицы.