ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "ВОЛГОГРАДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ"

Институт приоритетных технологий

Кафедра информационной безопасности

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины (модуля): **Нормативная и методическая документация по организации технической защиты информации**

Уровень ОПОП: Специалитет

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Безопасность компьютерных систем и сетей (по отрасли или в сфере профессиональной деятельности)

Форма обучения: Очная

Срок обучения: 2024 - 2030 уч. г.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.01 Компьютерная безопасность (приказ № 1459 от 26.11.2020 г.) и учебного плана, утвержденного Ученым советом (от 26.05.2023 г., протокол № 9)

Разработчики:
Радченко Д. П., старший преподаватель

Программа рассмотрена и утверждена на заседании кафедры, протокол № 08 от 30.08.2023 года

Зав. кафедрой Какорина О. А.

1. Цель и задачи изучения дисциплины

Цель изучения дисциплины - Целью освоения дисциплины является теоретическая и практическая подготовка выпускника в области организации информационной безопасности автоматизированных систем, а также контроля (аудита) ее эффективности.

Задачи освоения дисциплины:

Задачи дисциплины:

- Формирование навыков в организации проверки работоспособности применяемых средств защиты информации и выявления недостатков в их настройке и эксплуатации
- Формирование умений по разработке политики информационной безопасности и документации на систему защиты информации
- Формирование навыков в организации системы защиты информации
- Формирование специальных теоретических и практических знаний, обеспечивающих возможность организации информационной безопасности автоматизированных систем, а также контроля (аудита) ее эффективности

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Нормативная и методическая документация по организации технической защиты информации» относится к части учебного плана, формируемой участниками образовательных отношений.

Дисциплина изучается на 4 курсе.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование компетенций, определенных учебным планом в соответствии с ФГОС ВО.

Выпускник должен обладать следующими профессиональными компетенциями (ПК) в соответствии с видами деятельности:

- ПК-1 Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей

Знания, умения, навыки, формируемые по компетенции в рамках дисциплины

Студент должен знать:

знать основы формирования политики информационной безопасности; основные принципы и методы комплексной защиты информации.

принципы построения компьютерных систем и сетей; модели безопасности компьютерных систем; виды политик безопасности компьютерных систем и сетей политики безопасности компьютерных систем и сетей

архитектуру аппаратных, программных и программноаппаратных средств администрируемой сети

Студент должен уметь:

уметь выявлять угрозы информационной безопасности объектов информатизации, формировать политику информационной безопасности; подбирать меры и средства обеспечения информационной безопасности на объекте защиты

анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия;

разрабатывать профили защиты компьютерных систем; формулировать задания по безопасности компьютерных систем

Студент должен владеть навыками:

владеть навыками выявления угроз информации ограниченного доступа; разработки требований информационной безопасности к объектам информатизации.

выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации

- ПК-4 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности

Знания, умения, навыки, формируемые по компетенции в рамках дисциплины

Студент должен знать:

принципы и порядок работы информационно-справочных систем; способы поиска и обработки информации, методы работы с научной информацией, принципы и правила построения суждений и оценок

Студент должен уметь:

обобщать, анализировать и систематизировать научную информацию в области информационной безопасности; различать факты, интерпретации, оценки и аргументировано отстаивать свою позицию в процессе коммуникации; пользоваться информационно-справочными системами

Студент должен владеть навыками:

навыком составления и оформления реферата по результатам обзора научно-технической литературы, нормативных и методических документов

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Восьмой семестр
Контактная работа (всего)	**68**	**68**
Лекции	34	34
Практические	34	34
Самостоятельная работа (всего)	**40**	**40**
Виды промежуточной аттестации		
Зачет с оценкой		+
Общая трудоемкость часы	**108**	**108**
Общая трудоемкость зачетные единицы	**3**	**3**

5. Содержание дисциплины

5.1. Содержание дисциплины: Лекции (34 ч.)

Восьмой семестр. (34 ч.)

Тема 1. Цели и задачи ТЗИ (2 ч.)

Основные термины и определения в области ТЗИ. Место ТЗИ в системе мероприятий по обеспечению информационной безопасности в Российской Федерации.

Тема 2. Основы нормативного правового обеспечения ТЗИ (2 ч.)

Нормативные правовые акты Российской Федерации. Нормативные правовые акты ФСТЭК России. Методические документы. Технические документы (документация). Система сертификации средств защиты информации. Ответственность за правонарушения в области защиты информации.

Тема 3. Планирование работ по ТЗИ (2 ч.)

Организация и проведение работ по обеспечению ТЗИ на объектах информатизации. Порядок разработки, согласования и утверждения планов проведения мероприятий по ТЗИ.

Тема 4. Технические каналы утечки информации (2 ч.)

Нормативные правовые акты, методические документы, международные и национальные стандарты в области ТЗИ, цели и задачи ТЗИ. Термины и определения в области ТЗИ от утечки по техническим каналам: объект информатизации, защищаемое помещение, основные технические средства и системы (ОТСС), вспомогательные технические средства и системы (ВТСС), случайные антенны, контролируемая зона, ТКУИ.

Тема 5. Способы и средства защиты информации от утечки за счет ПЭМИН (2 ч.)

Способы и средства защиты информации, обрабатываемой техническими средствами, от утечки за счет побочных электромагнитных излучений и наводок. Классификация способов и средств защиты информации, обрабатываемой техническими средствами, от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН).

Тема 6. Меры и средства ТЗИ от НСД (2 ч.)

Организация и содержание проведения работ по ТЗИ от НСД, состав и содержание необходимых документов. Общая характеристика и классификация мер и средств защиты информации от НСД. Требования к мерам защиты информации от НСД, реализуемым в автоматизированной (информационной) системе. Меры защиты информации от НСД. Средства защиты информации от НСД.

Тема 7. Организация защиты информации на объектах информатизации (2 ч.)

Организация работ по созданию и эксплуатации объектов информатизации и их систем защиты информации. Положение о порядке организации и проведения работ по защите конфиденциальной информации. Перечень сведений конфиденциального характера, подлежащих защите.

Тема 8. Организация защиты информации на объектах информатизации (2 ч.)

Реализация требований по защите акустической речевой конфиденциальной информации и информации, обрабатываемой в средствах вычислительной техники от утечки по техническим каналам. Реализация требований по защите информации от НСД и специальных воздействий на эксплуатируемом (функционирующем) объекте информатизации. Реализация требований по защите информации от НСД и специальных воздействий при создании нового объекта информатизации в защищенном исполнении. Особенности реализации требований по защите персональных данных.

Тема 9. Проектирование систем защиты информации (2 ч.)

Создание и функционирование систем защиты конфиденциальной информации, как составные части работ по созданию и эксплуатации объектов информатизации учреждений и предприятий. Стадии и этапы создания систем защиты конфиденциальной информации. Порядок выполнения работ по защите информации о создаваемой автоматизированной системе в защищенном исполнении.

Тема 10. Проектирование систем защиты информации (2 ч.)

Комплекс работ по созданию системы защиты информации (формирование требований к системе защиты информации; разработка (проектирование) системы защиты информации; внедрение системы защиты информации; аттестация объекта информатизации по требованиям безопасности информации и ввод его в действие; сопровождение системы защиты информации в ходе эксплуатации объекта информатизации).

Тема 11. Проектирование систем защиты информации (2 ч.)

Разработка рабочей и эксплуатационной документации на систему защиты информации объекта информатизации (защищаемого помещения), а также организационно¬распорядительной документации по защите информации на объекте информатизации.

Тема 12. Организация аттестации объектов информатизации на соответствие требованиям безопасности информации (2 ч.)

Организационно-правовые основы системы аттестации объектов информатизации по требованиям безопасности информации. Цели и виды аттестации объектов информатизации на соответствие требованиям безопасности информации. Участники аттестации и их полномочия (компетенции). Требования к органам по аттестации объектов информатизации. Деятельность аттестационных комиссий. Сводный реестр сертифицированной продукции, используемой в целях защиты информации на аттестованных объектах информатизации. Государственный контроль (надзор) за соблюдением порядка аттестации и эксплуатацией аттестованных объектов информатизации.

Тема 13. Организация и выполнение мероприятий по аттестации объектов информатизации по требованиям безопасности информации (2 ч.)

Основные мероприятия по проведению аттестации объектов информатизации на соответствие

требованиям безопасности информации (подача и рассмотрение заявки на аттестацию объектов информатизации; предварительное ознакомление с аттестуемым объектом информатизации; разработка программ и методик аттестационных испытаний; проведение аттестационных испытаний объектов информатизации; оформление, регистрация и выдача аттестата соответствия).

Тема 14. Организация и выполнение мероприятий по аттестации объектов информатизации по требованиям безопасности информации (2 ч.)

Требования к разработке, структуре, оформлению и утверждению программ и методик аттестационных испытаний объектов информатизации (требования к содержанию программ и методик аттестационных испытаний автоматизированных систем, защищаемых помещений). Требования обеспечения защиты конфиденциальной информации при проведении аттестации объектов информатизации.

Тема 15. Организация и выполнение мероприятий по аттестации объектов информатизации по требованиям безопасности информации (2 ч.)

Методы проверки и испытаний, применяемые при проведении аттестационных испытаний (экспертно-документальный метод; измерение и оценка уровней , ПЭМИН для отдельных технических средств автоматизированной системы и каналов утечки информации; проверка функций или комплекса функций защиты информации от НСД с помощью тестирующих средств, а также путем пробного пуска средств защиты информации от НСД и наблюдения за их выполнением; попытки «взлома систем защиты информации»).

Тема 16. Организация и выполнение мероприятий по аттестации объектов информатизации по требованиям безопасности информации (2 ч.)

Разработка заключения и протоколов испытаний по результатам аттестации объектов информатизации. Оформление, регистрация и выдача «Аттестата соответствия». Ввод в действие и эксплуатация аттестованных по требованиям безопасности информации объектов информатизации. Состав и содержание документов, разрабатываемых для проведения аттестации и по результатам аттестации объектов информатизации. Вывод из эксплуатации аттестованных по требованиям безопасности информации объектов информатизации.

Тема 17. Основы организации контроля состояния ТЗИ (2 ч.)

Основные задачи контроля состояния ТЗИ. Нормативные и методические документы по контролю ТЗИ. Организация и порядок проведения контроля состояния ТЗИ. Методы и средства контроля защищенности конфиденциальной информации от НСД. Методы и средства контроля защищенности конфиденциальной информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН.

5.2. Содержание дисциплины: Практические (34 ч.)

Восьмой семестр. (34 ч.)

Тема 1. Формирование требований к системе защиты информации (2 ч.)

Формирование требований к средствам и системам информатизации в защищенном исполнении.

Тема 2. Проектирование средств и систем информатизации (2 ч.)

Проектирование средств и систем информатизации в защищенном исполнении

Тема 3. Разработка технического задания (2 ч.)

Разработка технического задания на создание системы защиты информации объекта информатизации.

Тема 4. Разработка эскизного проекта (2 ч.)

Разработка эскизного проекта системы защиты информации объекта информатизации

Тема 5. Разработка технического проекта (2 ч.)

Разработка технического проекта системы защиты информации объекта информатизации

Тема 6. Разработка рабочей и эксплуатационной документации (2 ч.)

Разработка рабочей и эксплуатационной документации на систему защиты информации объекта информатизации.

Тема 7. Разработка организационно-распорядительной документации (2 ч.)

Разработка организационно-распорядительной документации по защите информации на объекте информатизации

Тема 8. Определение технических каналов утечки информации (2 ч.)

Определение возможных ТКУИ на объектах информатизации

Тема 9. Разработка программ и методик аттестационных испытаний (2 ч.)

Разработка программ и методик аттестационных испытаний объектов информатизации на соответствие требованиям по защите информации от утечки по техническим каналам за счет ПЭМИН.

Тема 10. Разработка программ и методик аттестационных испытаний (2 ч.)

Разработка программ и методик аттестационных испытаний объектов информатизации на соответствие требованиям по защите информации от НСД.

Тема 11. Разработка программ и методик аттестационных испытаний (2 ч.)

Разработка программ и методик аттестационных испытаний объектов информатизации на соответствие требованиям по защите информации от утечки акустической речевой информации.

Тема 12. Мониторинг информационной безопасности средств и систем информатизации (2 ч.)

Порядок и методы мониторинга информационной безопасности средств и систем информатизации. Мониторинг парольной защиты и контроль надежности пользовательских паролей. Мониторинг попыток несанкционированного доступа. Контроль за событиями безопасности и действиями пользователей в средствах и системах информатизации.

Тема 13. Контроль защищенности информации (2 ч.)

Проведение контроля защищенности информации, обрабатываемой техническими средствами, от утечки за счет ПЭМИН с использованием программно-аппаратных комплексов.

Тема 14. Контроль защищенности информации (2 ч.)

Проведение контроля защищенности акустической речевой конфиденциальной информации от утечки по техническим каналам с использованием программно-аппаратных комплексов.

Тема 15. Контроль защищенности информации (2 ч.)

Проведение контроля защищенности конфиденциальной информации от НСД.

Тема 16. Контроль защищенности информации (2 ч.)

Документирование процедур и результатов контроля за обеспечением уровня защищенности информации, содержащейся в средствах и системах информатизации. Разработка предложений (рекомендаций) по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о модернизации систем защиты информации систем информатизации, повторной оценке эффективности систем защиты информации систем информатизации или проведении дополнительных работ по оценке
эффективности систем защиты информации систем информатизации

Тема 17. Аттестационные испытания (2 ч.)

Проведения аттестационных испытаний. Проверка выполнения требований по результатам аттестационных испытаний, разработка заключения по результатам аттестационных испытаний (аттестата соответствия). Оформление, регистрация и выдача «Аттестата соответствия».

6. Виды самостоятельной работы студентов по дисциплине

Восьмой семестр (40 ч.)

Вид СРС: Ознакомление с нормативными документами (40 ч.)

Тематика заданий СРС:

Нормативные документы:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

4. Федеральный закон от 4 мая 2011г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
5. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
6. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
7. Положение о лицензировании деятельности по технической защите конфиденциальной информации.
8. Положение о лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации
9. Положение о сертификации средств защиты информации
10. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
11. Требования к защите персональных данных при их обработке в информационных системах персональных данных. Утверждены постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.
12. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
13. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.

7. Тематика курсовых работ(проектов)

Курсовые работы (проекты) по дисциплине не предусмотрены.

8. Фонд оценочных средств. Оценочные материалы

8.1. Показатели и критерии оценивания компетенций, шкалы оценивания

В рамках изучаемой дисциплины студент демонстрирует уровни овладения компетенциями:

Повышенный уровень:

обучающийся демонстрирует глубокое знание учебного материала; способен использовать сведения из различных источников для успешного исследования и поиска решения в нестандартных ситуациях; способен анализировать, проводить сравнение и обоснование выбора методов решения практико-ориентированных заданий

Базовый уровень:

обучающийся способен понимать и интерпретировать освоенную информацию; демонстрирует осознанное владение учебным материалом и учебными умениями, навыками и способами деятельности, необходимыми для решения практико-ориентированных заданий

Пороговый уровень:

обучающийся обладает необходимой системой знаний и владеет некоторыми умениями; демонстрирует самостоятельность в применении знаний, умений и навыков к решению учебных заданий на репродуктивном уровне

Уровень ниже порогового:

система знаний, необходимая для решения учебных и практико-ориентированных заданий, не сформирована; обучающийся не владеет основными умениями, навыками и способами деятельности

Уровень сформированности компетенции	Шкала оценивания для промежуточной аттестации	Шкала оценивания по БРС
	Экзамен, зачет с оценкой	
Повышенный	5 (отлично)	91 и более

Базовый	4 (хорошо)	71 – 90
Пороговый	3 (удовлетворительно)	60 – 70
Ниже порогового	2 (неудовлетворительно)	Ниже 60

Критерии оценки знаний студентов по дисциплине

Оценка	Показатели
Отлично	Обучающийся демонстрирует: систематизированные, глубокие и полные знания по всем разделам учебной дисциплины, а также по основным вопросам, выходящим за ее пределы; точное использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы; безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении научных и профессиональных задач; выраженную способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации; полное и глубокое усвоение основной, и дополнительной литературы, по изучаемой учебной дисциплине; умение свободно ориентироваться в теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку, использовать научные достижения других дисциплин; творческую самостоятельную работу на учебных занятиях, активное творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.
Хорошо	Обучающийся демонстрирует: систематизированные, глубокие и полные знания по всем разделам учебной дисциплины; использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы и обобщения; владение инструментарием учебной дисциплины (методами комплексного анализа, техникой информационных технологий), умение его использовать в постановке и решении научных и профессиональных задач; способность решать сложные проблемы в рамках учебной дисциплины; свободное владение типовыми решениями; усвоение основной и дополнительной литературы, рекомендованной рабочей программой по учебной дисциплине; умение ориентироваться в теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку; активную самостоятельную работу на учебных занятиях, систематическое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

Удов-летвори-тельно	Обучающийся демонстрирует: достаточные знания в объеме рабочей программы по учебной дисциплине; использование научной терминологии, грамотное, логически правильно изложение ответа на вопросы, умение делать выводы без существенных ошибок; владение инструментарием учебной дисциплины, умение его использовать в решении учебных и профессиональных задач; способность самостоятельно применять типовые решения в рамках изучаемой дисциплины; усвоение основной литературы, рекомендованной рабочей программой по дисциплине; умение ориентироваться в базовых теориях, концепциях и направлениях по дисциплине; работу на учебных занятиях под руководством преподавателя, фрагментарное участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.
Неудов-летвори-тельно	Обучающийся демонстрирует: фрагментарные знания в рамках изучаемой дисциплины; знания отдельных литературных источников, рекомендованных рабочей программой по учебной дисциплине; неумение использовать научную терминологию учебной дисциплины, наличие в ответе грубых, логических ошибок; пассивность на занятиях или отказ от ответа, низкий уровень культуры исполнения заданий.

8.2. Вопросы, задания текущего контроля

В целях освоения компетенций, указанных в рабочей программе дисциплины, предусмотрены следующие вопросы, задания текущего контроля:

- ПК-1 Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей

Студент должен знать:

знать основы формирования политики информационной безопасности; основные принципы и методы комплексной защиты информации.

принципы построения компьютерных систем и сетей; модели безопасности компьютерных систем; виды политик безопасности компьютерных систем и сетей политики безопасности компьютерных систем и сетей

архитектуру аппаратных, программных и программноаппаратных средств администрируемой сети

Вопросы, задания:

1. Разработать политику по обеспечению ТЗИ на объекте информатизации.

2. Сформировать требования по обеспечению ТЗИ на объекте информатизации.

3. Требования по ТЗИ (нормы, требования и рекомендации по защите объектов информатизации, методы и методики контроля их выполнения).

Студент должен уметь:

уметь выявлять угрозы информационной безопасности объектов информатизации, формировать политику информационной безопасности; подбирать меры и средства обеспечения информационной безопасности на объекте защиты
анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия;
разрабатывать профили защиты компьютерных систем; формулировать задания по безопасности компьютерных систем

Задания:

1. Разработать модель угроз безопасности информации выбранного объекта информатизации.
2. Определить актуальные угрозы безопасности информации объекта информатизации.
3. Подобрать меры и средства защиты информации в соответствии с заданными требованиями безопасности.

Студент должен владеть навыками:

владеть навыками выявления угроз информации ограниченного доступа; разработки требований информационной безопасности к объектам информатизации.
выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации

Задания:

1. Сформировать требования по защите акустической речевой конфиденциальной информации и информации, обрабатываемой в средствах вычислительной техники от утечки по техническим каналам.
2. Сформировать требования к системе защиты информации объекта информатизации.
3. Сформировать требования по защите информации объекта информатизации от НСД.

- ПК-4 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности

Студент должен знать:

принципы и порядок работы информационно-справочных систем; способы поиска и обработки информации, методы работы с научной информацией, принципы и правила построения суждений и оценок

Вопросы, задания:

1. С помощью Государственного реестра сертифицированных средств защиты информации подберите СЗИ для выбранного объекта информатизации.
2. С помощью Банка данных угроз безопасности информации ФСТЭК сформируйте перечень возможных угроз для выбранного объекта информатизации.
3. С помощью Банка данных угроз безопасности информации ФСТЭК подберите меры защиты от выделенных угроз для выбранного объекта информатизации.

Студент должен уметь:

обобщать, анализировать и систематизировать научную информацию в области информационной безопасности; различать факты, интерпретации, оценки и аргументировано отстаивать свою позицию в процессе коммуникации; пользоваться информационно-справочными системами

Задания:

1. Доступ к каким категориям информации нельзя ограничить в соответствии с федеральным законодательством? Назовите ФЗ о котором идет речь.
2. Каким нормативным документом утвержден Перечень сведений конфиденциального характера?

3. Какой документ устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных?

Студент должен владеть навыками:

навыком составления и оформления реферата по результатам обзора научно-технической литературы, нормативных и методических документов

Задания:

1. Что утверждает Постановление Правительства от 1 ноября 2012 г. № 1119? Опишите основные положения утвержденного документа.

2. Что определяет Порядок, утвержденный приказом ФСТЭК от 29 апреля 2021 г. N 77? Опишите основные положения Порядка.

3. Какие требования утверждены приказом ФСТЭК от 29 апреля 2021 г. N 77? Опишите основные положения утвержденного документа.

8.3. Вопросы промежуточной аттестации

Восьмой семестр (Зачет с оценкой)

1. Место ТЗИ в системе мероприятий по обеспечению информационной безопасности в Российской Федерации

2. Цели и задачи ТЗИ.

3. Объекты информатизации: классификация и характеристика.

4. Нормативные правовые акты ФСТЭК России.

5. Требования по защите конфиденциальной информации, обрабатываемой в автоматизированных (информационных) системах.

6. Требования по защите акустической речевой информации.

7. Требования по защите персональных данных.

8. Организация и проведение работ по обеспечению ТЗИ на объектах информатизации.

9. Стадии создания системы защиты информации объекта информатизации.

10. Формирование требований к средствам и системам информатизации в защищенном исполнении.

11. Порядок проектирования средств и систем информатизации в защищенном исполнении.

12. Аттестация объекта информатизации по требованиям безопасности информации и ввод его в действие.

13. Сопровождение системы защиты информации в ходе эксплуатации объекта информатизации.

14. Разработка эксплуатационной документации на систему защиты информации.

8.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Промежуточная аттестация обучающихся ведется непрерывно и включает в себя:

для дисциплин, завершающихся (согласно учебному плану) зачетом/зачетом с оценкой (дифференцированным зачетом), – текущую аттестацию (контроль текущей работы в семестре, включая оценивание промежуточных результатов обучения по дисциплине, – как правило, по трем модулям) и оценивание окончательных результатов обучения по дисциплине;

для дисциплин, завершающихся (согласно учебному плану) экзаменом, – текущую аттестацию (контроль текущей работы в семестре, включая оценивание промежуточных результатов обучения по дисциплине, – как правило, по трем модулям) и семестровую аттестацию (экзамен) – оценивание окончательных результатов обучения по дисциплине.

По дисциплинам, завершающимся зачетом/зачетом с оценкой, по обязательным формам текущего контроля студенту предоставляется возможность набрать в сумме не менее 100 баллов.

Оценивание окончательных результатов обучения по дисциплине ведется по 100-балльной шкале, оценка формируется автоматически как сумма количества баллов, набранных обучающимся за выполнение заданий обязательных форм текущего контроля.

По дисциплинам, завершающимся экзаменом, по обязательным формам текущего контроля студенту предоставляется возможность набрать в сумме не менее 60 баллов.

Оценивание окончательных результатов обучения по дисциплине ведется по 100-балльной шкале, оценка формируется автоматически как сумма количества баллов, набранных обучающимся за выполнение заданий обязательных форм текущего контроля и количества баллов, набранных на семестровой аттестации (экзамене).

Система оценивания.

В соответствии с Положением о балльно-рейтинговой системе оценки успеваемости обучающихся Волгоградского государственного университета предусмотрена возможность предоставления студентам выполнения дополнительных заданий повышенной сложности (не включаемых в перечень обязательных и, соответственно, в перечень обязательного текущего контроля успеваемости) и получения за выполнение таких заданий «премиальных» баллов, - для поощрения обучающихся, демонстрирующих выдающие способности.

Оценка качества освоения образовательной программы включает текущий контроль успеваемости, промежуточную аттестацию обучающихся и государственную итоговую аттестацию выпускников.

Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на протяжении семестра. К основным формам текущего контроля можно отнести:

Форма текущего контроля: Контрольная работа

контрольные работы применяются для оценки знаний, умений, навыков по дисциплине или ее части. Контрольная работа, как правило, состоит из небольшого количества средних по трудности вопросов, задач или заданий, требующих поиска обоснованного ответа. Может занимать часть или полное учебное занятие с разбором правильных решений на следующем занятии.

Форма текущего контроля: Устный опрос, собеседование

устный опрос, собеседование являются формой оценки знаний и предполагают специальную беседу преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной. Процедуры направлены на выяснение объема знаний, обучающегося по определенному разделу, теме, проблеме и т.п.

Форма текущего контроля: Письменные задания или лабораторные работы

письменные задания являются формой оценки знаний и предполагают подготовка письменного ответа, решение специализированной задачи, выполнение теста. являются формами контроля и средствами применения и реализации полученных обучающимися знаний, умений и навыков в ходе выполнения учебно-практической задачи, связанной с получением значимого результата с помощью реальных средств деятельности. Рекомендуются для проведения в рамках тем (разделов), наиболее значимых в формировании компетенций. Тест является простейшей формой контроля, направленной на проверку владения терминологическим аппаратом, современными информационными технологиями и конкретными знаниями в области фундаментальных и прикладных дисциплин. Тест состоит из небольшого количества элементарных задач; может предоставлять возможность выбора из перечня ответов; занимает часть учебного занятия (10–30 минут); правильные решения разбираются на том же или следующем занятии; частота тестирования определяется преподавателем.

Промежуточная аттестация, как правило, осуществляется в конце семестра и может завершать изучение, как отдельной дисциплины, так и ее раздела (разделов) /модуля (модулей). Промежуточная аттестация помогает оценить более крупные совокупности знаний, умений и навыков, в некоторых случаях – даже формирование определенных компетенций.

К формам промежуточного контроля можно отнести:

Форма промежуточной аттестации: Зачет с оценкой

зачет с оценкой служит формой проверки усвоения учебного материала по дисциплине (модулю), практики, готовности к практической деятельности.

Методика формирования результирующей оценки:

Восьмой семестр

1. Контрольная работа - от 0 до 30 баллов
2. Устный опрос, собеседование - от 0 до 10 баллов
3. Письменные задания или лабораторные работы - от 0 до 60 баллов
4. Зачет с оценкой - Аттестация по дисциплине в форме зачета (зачета с оценкой) проводится по сумме результатов модульных контрольных работ и текущей успеваемости обучающегося.

9. Перечень основной и дополнительной учебной литературы

9.1 Основная литература

1. Партыка Татьяна Леонидовна Информационная безопасность [Электронный ресурс]: учебное - Издание перераб. и доп. - ФОРУМ, 2019. - 432 с. - Режим доступа: http://new.znanium.com/go.php?id=987326

9.2 Дополнительная литература

1. Баранова Елена Константиновна Информационная безопасность и защита информации [Электронный ресурс]: учебное - Издание 3 - РИОР, 2017. - 322 с. - Режим доступа: http://new.znanium.com/go.php?id=763644

2. Гришина Наталия Васильевна Информационная безопасность предприятия [Электронный ресурс]: учебное - Издание доп. - ФОРУМ, 2017. - 239 с. - Режим доступа: http://new.znanium.com/go.php?id=612572

В качестве учебно-методического обеспечения могут быть использованы другие учебные, учебно-методические и научные источники по профилю дисциплины, содержащиеся в электронно-библиотечных системах, указанных в п. 11.2 «Электронно-библиотечные системы».

9.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. http://fstec.ru - Официальный сайт Федеральной службы по техническому и экспортному контролю
2. http://lib.volsu.ru - Электронная библиотека Волгоградского государственного университета
3. http://window.edu.ru/library - Федеральный образовательный портал. Библиотека. Единое окно доступа к образовательным ресурсам
4. http://new.volsu.ru/umnik - Образовательный портал Волгоградского государственного университета «УМНИК»

10.Методические указания по освоению дисциплины для лиц с ОВЗ и инвалидов

При необходимости обучения студентов-инвалидов и лиц с ограниченными возможностями здоровья аудиторные занятия могут быть заменены или дополнены изучением полнотекстовых лекций, презентаций, видео- и аудиоматериалов в электронной информационно-образовательной среде (ЭИОС) университета. Индивидуальные задания подбираются в адаптированных к ограничениям здоровья формах (письменно или устно, в форме презентаций). Выбор методов обучения зависит от их доступности для инвалидов и лиц с ограниченными возможностями здоровья.

В целях реализации индивидуального подхода к обучению студентов, осуществляющих учебный процесс по индивидуальной траектории в рамках индивидуального учебного плана (при необходимости), изучение данной дисциплины базируется на следующих возможностях:
- индивидуальные консультации преподавателя;
- максимально полная презентация содержания дисциплины в ЭИОС (в частности, полнотекстовые лекции, презентации, аудиоматериалы, тексты для перевода и анализа и т.п.).

11. Перечень информационных технологий

В учебном процессе активно используются информационные технологии с применением современных средств телекоммуникации; электронные учебники и обучающие компьютерные программы. Каждый обучающийся обеспечен неограниченным доступом к электронной информационно-образовательной среде (ЭИОС) университета. ЭИОС предоставляет открытый доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к электронным библиотечным системам и электронным образовательным ресурсам.

11.1 Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)

Аудитория 2-30 К
Лицензионное программное обеспечение:
1. 7-zip – свободно-распространяемое программное обеспечение;
2. Microsoft Windows 7 – лицензия No 49487352;
3. Microsoft Office 2007 – лицензия No 44414438;
4. Антивирус Kaspersky – P/N: KL4863RAUFQ;
5. Adobe Acrobat Reader – открытая лицензия

Аудитория 2-29 К
Программное обеспечение:
1. 7-zip, 1 лицензия GNU LGPL свободное программное обеспечение
2. Microsoft Windows 7 Home Premium, 1 OEM-лицензии
3. Microsoft Office 2007 Standart, 1 лицензия, номер 43847745
4. Антивирус Kaspersky Endpoint Security, 1 лицензия, номер 500999

11.2 Современные профессиональные базы данных и информационно-справочные системы, в т.ч. электронно-библиотечные системы
(обновление выполняется еженедельно)

Название	Краткое описание	URL-ссылка
Научная электронная библиотека	Крупнейший российский информационный портал в области науки, технологии, медицины и образования.	http://elibrary.ru/
ЭБС "Лань"	Электронно-библиотечная система	https://e.lanbook.com/
ЭБС Znanium.com	Электронно-библиотечная система	https://znanium.com/
ЭБС BOOK.ru	Электронно-библиотечная система	https://www.book.ru/
ЭБС Юрайт	Электронно-библиотечная система	https://www.biblio-online.ru/
Scopus	Scopus – крупнейшая единая база данных, содержащая аннотации и информацию о цитируемости рецензируемой научной литературы, со встроенными инструментами отслеживания, анализа и визуализации данных. В базе содержится 23700 изданий от 5000 международных издателей, в области естественных, общественных и гуманитарных наук, техники, медицины и искусства.	http://www.scopus.com/

Web of Science	Наукометрическая реферативная база данных журналов и конференций. С платформой Web of Science вы можете получить доступ к непревзойденному объему исследовательской литературы мирового класса, связанной с тщательно отобранным списком журналов, и открыть для себя новую информацию при помощи скрупулезно записанных метаданных и ссылок.	https://apps.webofknowledge.com/
КонсультантПлюс	Информационно-справочная система	http://www.consultant.ru/
Гарант	Информационно-справочная система по законодательству Российской Федерации	http://www.garant.ru/
Научная библиотека ВолГУ им О.В. Иншакова		http://library.volsu.ru/

12. Материально-техническое обеспечение дисциплины

Аудитория 2-30 К
Специализированная мебель:
парта со скамьей- 52 шт.
учебные места - 104 шт.
рабочее место преподавателя (стол и стул) – 1 шт.
доска аудиторная-1 шт.
Демонстрационное оборудование:
1. Доска (магнитная, маркерная)
2. Проектор Epson EMP-X52
3. Экран для проектора
Технические средства обучения:
Ноутбук ACER AspireES1-523-294D, 15.6", AMDE1 7010
1.5ГГц, 4ГБ, 500ГБ, AMDRadeonR2
Аудитория 2-29 К
Специализированная мебель:
парта со скамьей- 20 шт.
учебные места - 40 шт.
рабочее место преподавателя (парта со скамьей) – 1 шт.
Демонстрационное оборудование:
1. Доска (магнитная, меловая)
2. Проектор BenQ MX 505
3. Экран для проектора
Технические средства обучения:
1. Ноутбук 15,6” ASUS P53S/P53SJ, Intel Core i5