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

Институт приоритетных технологий

Кафедра информационной безопасности

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины (модуля): **Теория информационной безопасности и методология 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:
Топилин Я. Н., кандидат социологических наук, доцент

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 - является важной составляющей общей профессиональной подготовки специалистов в области обеспечения информационной безопасности. Целями дисциплины являются раскрытие сущности и значения информационной безопасности и защиты информации, концептуальных, методологических и организационных основ обеспечения безопасности информации, классификация и характеристики составляющих информационной безопасности и защиты информации, установление взаимосвязи и логической организации входящих в нее компонентов.

Задачи дисциплины:

- ознакомление с понятийным аппаратом в области информационной безопасности и защиты информации;
- рассмотрение базовых содержательных положений в области информационной безопасности и защиты информации;
- изучение современной доктрины информационной безопасности;
- определение целей и принципов защиты информации;
- установление факторов, влияющих на защиту информации;
- ознакомление с составом защищаемой информации, ее классификацией по видам тайны, материальным носителям, собственникам и владельцам;
- установление структуры угроз защищаемой информации;
- определение сущности компонентов защиты информации;
- определение назначения, сущности и структуры систем защиты информации.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Теория информационной безопасности и методология защиты информации» относится к обязательной части учебного плана.

Дисциплина изучается на 3 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 общепрофессиональными компетенциями (ОПК):

- ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспертному контролю

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

Студент должен знать:

систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; систему организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; основные угрозы безопасности информации и модели нарушителя объекта информатизации

Студент должен уметь:

разрабатывать модели угроз и модели нарушителя объекта информатизации; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации

Студент должен владеть навыками:

навыками разработки проектов нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации

- ОПК-8 Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей

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

Студент должен знать:

методологию научного исследования для определения параметров и характеристик средств защиты информации

Студент должен уметь:

применять исследовательский подход в процессе сертификации средств защиты информации

Студент должен владеть навыками:

навыком и практическим опытом проведения научного исследования в процессе сертификации средств защиты информации

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Пятый семестр
Контактная работа (всего)	**50**	**50**
Лабораторные	16	16
Лекции	34	34
Самостоятельная работа (всего)	**22**	**22**
Виды промежуточной аттестации	**36**	**36**
Экзамен	36	36
Общая трудоемкость часы	**108**	**108**
Общая трудоемкость зачетные единицы	**3**	**3**

5. Содержание дисциплины

5.1. Содержание дисциплины: Лабораторные (16 ч.)

Пятый семестр. (16 ч.)

Тема 1. Методы оценивания угроз безопасности в информационных системах. (2 ч.)

На основе методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных оценить угрозы утечки информации по каналу побочных электромагнитных излучений и наводок (ПЭМИН) (из-за наличия электромагнитных излучений, в основном, монитора и системного блока компьютера).

Тема 2. Методы оценивания угроз безопасности в информационных системах. (2 ч.)

На основе методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных оценить угрозы внедрения вредоносных программ.

Тема 3. Методы оценивания угроз безопасности в информационных системах. (2 ч.)

На основе методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных оценить угрозы утечки акустической (речевой) информации (возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, возможно при наличии функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн).

Тема 4. Модели безопасности на основе дискреционной политики. (2 ч.)

Пятимерное пространство Хартсона. Модель Харрисона-Руззо-Ульмана.

Тема 5. Субъектно-объектная модель компьютерной системы в механизмах и процессах коллективного доступа к информационным ресурсам. (2 ч.)

Субъектно-объектная модель компьютерной системы в механизмах и процессах коллективного доступа к информационным ресурсам.

Тема 6. Модели безопасности на основе мандатной политики. (2 ч.)

Модель Белла-ЛаПадулы. Основные расширения модели Белла-ЛаПадулы.

Тема 7. Дискреционная модель HRU (2 ч.)

Составление матрицы доступа к информационным ресурсам АС.

Тема 8. Модель распространения прав доступа Take-Grant. (2 ч.)

Модель распространения прав доступа Take-Grant.

5.2. Содержание дисциплины: Лекции (34 ч.)

Пятый семестр. (34 ч.)

Тема 1. Основы теории информационной безопасности. (2 ч.)

Анализ основных нормативно правовых документов по обработке и защите информации.

Тема 2. Основные понятия информационной безопасности и защиты информации. (2 ч.)

ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения.

Тема 3. Угрозы безопасности информации в информационных системах. (2 ч.)

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. Федеральной службой по техническому и экспортному контролю 15 февраля 2008 г.). Классификация угроз безопасности персональных данных. Угрозы утечки информации по техническим каналам. Угрозы утечки акустической (речевой) информации. Угрозы утечки видовой информации. Угрозы утечки информации по каналам побочных электромагнитных излучений и наводок. Угрозы несанкционированного доступа к информации

Тема 4. Методы оценивания угроз безопасности в информационных системах. (2 ч.)

Общая схема проведения моделирования угроз.Банк данных угроз безопасности ФСТЭК. Модели угроз безопасности ФСТЭК. Отраслевые модели угроз.

Тема 5. Субъектно-объектная модель компьютерной системы в механизмах и процессах коллективного доступа к информационным ресурсам. (2 ч.)

Субъект доступа.Объект доступа.Пользователь КС.Правила разграничения доступа субъектов к объектам.

Тема 6. Дискреционная модель HRU (2 ч.)

Модель HRU. Матрица доступа. Примитивный базис модели HRU.

Тема 7. Дискреционная модель HRU (2 ч.)

Монооперационные системы. Примеры построения базисов преобразования матрицы доступов.

Тема 8. Модель распространения прав доступа Take-Grant. (2 ч.)

Модель распространения прав доступа Take-Grant. Граф доступов и правила его преобразования. Формальное описание модели Take-Grant.

Тема 9. Модель распространения прав доступа Take-Grant. (2 ч.)

Возможность похищения прав доступа. Расширенная модель “Take-Grant”

Тема 10. Мандатная модель Белла-Лападула. (2 ч.)

Мандатная модель Белла-Лападула. Правила модели Белла-ЛаПадулы.

Тема 11. Мандатная модель Белла-Лападула. (2 ч.)

Безопасность в смысле Белла-Ла Падулы.Примеры типовых задач.

Тема 12. Модель тематического разграничения доступа на основе иерархических рубрикаторов. (2 ч.)

Модель тематического разграничения доступа на основе иерархических рубрикаторов.

Тема 13. Модель тематического разграничения доступа на основе иерархических рубрикаторов. (2 ч.)

Решетки в моделях тематического разграничения доступа. Решетка мультирубрик на иерархических рубрикаторах.

Тема 14. Модель ролевого доступа при иерархически организованной системы ролей. (2 ч.)

Базовая модель ролевого управления доступом. Базовая модель ролевого управления доступом.

Тема 15. Модель ролевого доступа при иерархически организованной системы ролей. (2 ч.)

Модель мандатного ролевого управления доступом. Защита от угрозы конфиденциальности информации.

Тема 16. Модель анализа индивидуально-групповых систем назначения доступа к иерархически организованным объектам доступа. (2 ч.)

Модель анализа индивидуально-групповых систем назначения доступа к иерархически организованным объектам доступа.

Тема 17. Пространственно-векторные модели комплексной оценки защищенности. (2 ч.)

Системы многомерного шкалирования защищенности компьютерных систем

6. Виды самостоятельной работы студентов по дисциплине

Пятый семестр (22 ч.)

Вид СРС: Подготовка рефератов (22 ч.)

Тематика заданий СРС:

Реферат – письменная работа объемом 8–10 страниц. Это краткое и точное изложение сущности какого-либо вопроса, темы.

Тему реферата студент выбирает из предложенных преподавателем или может предложить свой вариант. В реферате нужны развернутые аргументы, рассуждения, сравнения. Содержание темы излагается объективно от имени автора.

Функции реферата. Информативная, поисковая, справочная, сигнальная, коммуникативная. Степень выполнения этих функций зависит от содержательных и формальных качеств реферата и целей.

Требования к языку реферата. Должен отличаться точностью, краткостью, ясностью и простотой.

Структура реферата.

1. Титульный лист.

2. Оглавление (на отдельной странице). Указываются названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата.

3. Введение. Аргументируется актуальность исследования, т.е. выявляется практическое и теоретическое значение данного исследования. Далее констатируется, что сделано в данной области предшественниками, перечисляются положения, которые должны быть обоснованы. Обязательно формулируются цель и задачи реферата.

4. Основная часть. Подчиняется собственному плану, что отражается в разделении текста на главы, параграфы, пункты. План основной части может быть составлен с использованием различных методов группировки материала. В случае если используется чья-либо неординарная мысль, идея, то обязательно нужно сделать ссылку на того автора, у кого взят данный материал.

5. Заключение. Последняя часть научного текста. В краткой и сжатой форме излагаются полученные результаты, представляющие собой ответ на главный вопрос исследования.

6. Приложение. Может включать графики, таблицы, расчеты.

7. Библиография (список литературы). Указывается реально использованная для написания реферата литература. Названия книг располагаются по алфавиту с указанием их выходных данных.

При проверке реферата оцениваются:
- знание фактического материала, усвоение общих представлений, понятий, идей;
- характеристика реализации цели и задач исследования;
- степень обоснованности аргументов и обобщений;
- качество и ценность полученных результатов;
- использование литературных источников;
- культура письменного изложения материала;
- культура оформления материалов работы.

Темы рефератов:
1. Определение информационной безопасности в свете информационных проблем современного общества
2. Основные составляющие информационной безопасности
3. Угрозы информационной безопасности

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:

- ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспертному контролю

Студент должен знать:

систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации; задачи органов защиты государственной тайны и служб защиты информации на предприятиях; систему организационных мер, направленных на защиту информации ограниченного доступа; нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа; основные угрозы безопасности информации и модели нарушителя объекта информатизации

Вопросы, задания:

1. Основныех нормативные правовые документы по обработке и защите информации.
2. Классификация угроз безопасности персональных данных.
3. Угрозы утечки информации по техническим каналам.

Студент должен уметь:

разрабатывать модели угроз и модели нарушителя объекта информатизации; разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации; определить политику контроля доступа работников к информации ограниченного доступа; формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации

Задания:

1. Составление матрицы доступа к информационным ресурсам АС.
2. Разработать модель нарушителя.
3. Оцените возможности реализации угроз и их актуальность в АС.

Студент должен владеть навыками:

навыками разработки проектов нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации

Задания:

1. Подготовить документ Разрешительная система доступа к информационным ресурсам автоматизированной системы.
2. Составить документ Описание технологического процесса обработки информации в автоматизированной системе.

3. Подготовить Акт классификации автоматизированной системы.

- ОПК-8 Способен применять методы научных исследований при проведении разработок в области обеспечения безопасности компьютерных систем и сетей

Студент должен знать:

методологию научного исследования для определения параметров и характеристик средств защиты информации

Вопросы, задания:

1. Какие функции безопасности должны быть реализованы в системе обнаружения вторжений?
2. Функциональные требования и требования доверия, которым должно удовлетворять средство антивирусной защиты.

Студент должен уметь:

применять исследовательский подход в процессе сертификации средств защиты информации

Задания:

1. Правовое обоснование сертификации средств защиты информации.

Студент должен владеть навыками:

навыком и практическим опытом проведения научного исследования в процессе сертификации средств защиты информации

Задания:

1. Составить план процесса сертификации согласно основным этапом сертификации.

8.3. Вопросы промежуточной аттестации

Пятый семестр (Экзамен)

1. Методы оценивания угроз безопасности в информационных системах.
2. Подходы, принципы, методы и средства обеспечения безопасности
3. Классификация угроз информационной безопасности.
4. Виды противников и каналы утечки информации.
5. Политика безопасности информационных систем.
6. Теоретико-графовые модели комплексной оценки защищенности КС. Технико-экономическое обоснование систем обеспечения безопасности.
7. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам. Итоговые права доступа.
8. Общая характеристика политики тематического разграничения доступа.
9. Решетки в моделях тематического разграничения доступа.
10. Решетка мульти рубрик на иерархических рубрикаторах.
11. Скрытые каналы утечки информации и теоретико-информационные модели безопасности.
12. Модели ролевого доступа.
13. Принципы наделения ролей полномочиями.
14. Модель Белла-ЛаПадулы и основная теорема безопасности.
15. Основные расширения модели Белла-ЛаПадулы.
16. Общая характеристика политики тематического разграничения доступа.
17. Основы политики мандатного доступа.
18. Дискреционные модели безопасности компьютерных систем.
19. Пятимерное пространство Хартсона.
20. Модели безопасности на основе матрицы доступа.
21. Способы организации матрицы доступа и управления доступом в компьютерных системах.

22. Дискреционные модели распространения прав доступа.
23. Модель и теоремы безопасности Харрисона-Руззо-Ульмана.

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: Экзамен

экзамен по дисциплине или ее части имеет цель оценить сформированность компетенций, теоретическую подготовку студента, его способность к творческому мышлению, приобретенные им навыки самостоятельной работы, умение синтезировать полученные знания и применять их при решении практических задач. Форма проведения, как правило, предусматривает ответы на вопросы экзаменационного билета, выполнение которых направленно на проверку сформированности компетенций по соответствующей учебной дисциплине.

Методика формирования результирующей оценки:

Пятый 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. Экзамен - от 0 до 40 баллов

9. Перечень основной и дополнительной учебной литературы

9.1 Основная литература

1. Внуков Андрей Анатольевич Основы информационной безопасности: защита информации [Электронный ресурс]: - Издание испр. и доп - Юрайт, 2019. - 240 с. - Режим доступа: https://urait.ru/bcode/431332

2. Шаньгин Владимир Федорович Информационная безопасность компьютерных систем и сетей [Электронный ресурс]: учебное - ФОРУМ, 2018. - 416 с. - Режим доступа: http://new.znanium.com/go.php?id=945331

3. Щеглов Андрей Юрьевич Защита информации: основы теории [Электронный ресурс]: - Юрайт, 2019. - 309 с. - Режим доступа: https://urait.ru/bcode/433715

9.2 Дополнительная литература

1. Жук Александр Павлович Защита информации [Электронный ресурс]: учебное - Издание 2 - РИОР, 2015. - 392 с. - Режим доступа: http://new.znanium.com/go.php?id=474838

2. Медведев, В. А. Информационная безопасность. Введение в специальность [Электронный ресурс]: учебное - КноРус, 2019. - 144 с. - Режим доступа: http://www.book.ru/book/930545

3. Шаньгин Владимир Федорович Информационная безопасность компьютерных систем и сетей [Электронный ресурс]: учебное - ФОРУМ, 2016. - 416 с. - Режим доступа: http://new.znanium.com/go.php?id=549989

4. Бирюков Андрей Александрович Информационная безопасность: защита и нападение [Электронный ресурс]: - Издание 2 - ДМК Пресс, 2017. - 434 с. - Режим доступа: http://znanium.com/go.php?id=1028060

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://elibrary.ru/ - ELIBRARY.RU
2. http://fstec.ru - Официальный сайт Федеральной службы по техническому и экспортному контролю
3. http://www.garant.ru/ - Гарант
4. http://www.consultant.ru/ - КонсультантПлюс
5. https://e.lanbook.com/ - ЭБС "Лань"
6. https://www.biblio-online.ru/ - ЭБС Юрайт
7. https://znanium.com/ - ЭБС Znanium.com
8. http://lib.volsu.ru - Электронная библиотека Волгоградского государственного университета

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
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Помещение обеспечено доступом к информационно-телекоммуникационной сети Интернет, в

электронную информационно-образовательную среду ФГАОУ ВО «ВолГУ» и к электронным библиотечным системам.
Специализированная мебель:
Парта со скамьей- 106 шт.
Учебные места - 260 шт.
Рабочее место преподавателя (стол и стул) – 3 шт.
Доска аудиторная-1 шт.
Технические средства обучения:
Компьютерный комплекс кафедры мультимедийной -1 шт.
Мультимедийная кафедра -1 шт.
Мультимедийный проектор (EIKI EK DLP Projector EK-625U) -1 шт.
Интерактивная доска-1 шт.
Перечень лицензионного и свободно распространяемого программного обеспечения*:
Microsoft Windows 10 PRO. Номер лицензии: 65946188
Microsoft Office профессиональный 2016. Номер лицензии: нет. Номер договора 31604241628.2016 от 21.11.2016 г.
Kaspersky Endpoint Security. Номер лицензии: 280E-201102-083042-350-950
7-zip-открытая лицензия
Adope Acrobat Reader – открытая лицензия
Учебно-наглядные пособия:
Брошюры:
1. Дискреционная политика безопасности
2. Мандатная политика безопасности
Аудитория 2-04 К
Аудитория 2-04 К
Лаборатория программных, программно-аппаратных средств защиты информации и обеспечения информационной безопасности (Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, лабораторного типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.)
Специализированная мебель:
1. компьютерные столы – 13 шт.
2. стулья – 29 шт.
3. парта – 8 шт.
4. рабочее место преподавателя (стол и стул) – 1 шт.
Средства вычислительной техники (15 шт):
1. Компьютерный комплекс Option в составе: Системный блок клавиатура, мышь, монитор (13 шт);
2. Ноутбук Acer AS5738G;
3. Ноутбук HP Pavilion экран 15,6” Intel Pentium N3540.
Сетевое оборудование:
1. Маршрутизатор ASUS WL-520GU.
2. Концентратор.
Демонстрационное оборудование:
1. Доска (магнитная, маркерная)
2. Проектор projector DLP ColorBoost II
3. Экран для проектора Digis
Программное обеспечение:
1. Windows 10 Профессиональная, 13 лицензий, номер 65946188.

2. Microsoft Windows 8.1 Home, 1 лицензия OEM-лицензия
3. Microsoft Office 2016, 14 лицензий, сублицензионный договор No31604241628 от 21.11.2016.
4. Oracle VM VirtualBox 15 лицензий GNU GPL свободное программное обеспечение
5. Microsoft Windows 7 Home Premium, 1 лицензия, OEM-лицензия
6. Microsoft Office 2007 Standart, 1 лицензия, номер 43847745

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- 106 шт.
Учебные места - 260 шт.
Рабочее место преподавателя (стол и стул) – 3 шт.
Доска аудиторная-1 шт.

Технические средства обучения:
Компьютерный комплекс кафедры мультимедийной -1 шт.
Мультимедийная кафедра -1 шт.
Мультимедийный проектор (EIKI EK DLP Projector EK-625U) -1 шт.
Интерактивная доска-1 шт
Аудитория 2-04 К
Специализированная мебель:
1. компьютерные столы – 13 шт.
2. стулья – 29 шт.
3. парта – 8 шт.
4. рабочее место преподавателя (стол и стул) – 1 шт.
Средства вычислительной техники (15 шт):
1. Компьютерный комплекс Option в составе: Системный блок клавиатура, мышь, монитор (13 шт);
2. Ноутбук Acer AS5738G;
3. Ноутбук HP Pavilion экран 15,6” Intel Pentium N3540.
Сетевое оборудование:
1. Маршрутизатор ASUS WL-520GU.
2. Концентратор.
Демонстрационное оборудование:
1. Доска (магнитная, маркерная)
2. Проектор projector DLP ColorBoost II
3. Экран для проектора Digis
.