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

Институт приоритетных технологий

Кафедра информационной безопасности

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование
дисциплины (модуля): **Основы информационной безопасности**

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:
Петрищева Т. С., кандидат экономических 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 - заложить методически правильные основы знаний, необходимые будущим
специалистам-практикам в области информационной безопасности.

Задачи дисциплины:

- изучение понятийного аппарата в области информационной безопасности;
- изучение требований нормативных правовых актов Российской Федерации, методических, руководящих и организационно-распорядительных документов в области информационной безопасности;
- изучение состава защищаемой информации, ее классификации по видам тайны, материальным носителям, собственникам и владельцам;
- изучение угроз защищаемой информации;
- приобретение навыков построения системы защиты информации.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Основы информационной безопасности» относится к обязательной части учебного плана.

Дисциплина изучается на 1 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-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства

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

Студент должен знать:

сущность и понятие информации, информационной безопасности, их роль в современном обществе, значение для обеспечения объективных потребностей личности общества и государства; психологические аспекты информационной безопасности в современном обществе; угрозы и источники угроз информационной
безопасности современного общества; основные методы обеспечения информационной безопасности оперировать базовой терминологией в области информационной безопасности личности, общества и государства, гуманитарных аспектов информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации

Студент должен уметь:

оперировать базовой терминологией в области информационных технологий, информационной безопасности личности, общества и государства, гуманитарных аспектов информационной безопасности.

Студент должен владеть навыками:

основными информационными технологиями, базовыми методами выявления и классификации угроз информационной безопасности современного общества, основными подходами к противодействию угроз информационной безопасности

- ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

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

Студент должен знать:

основные нормативные правовые акты в области информационной безопасности и защиты информации, нормативные и методические документы Федеральной службы безопасности по техническому и экспортному контролю в данной области

Студент должен уметь:

применять нормативные правовые акты в своей профессиональной деятельности

Студент должен владеть навыками:

навыками работы с нормативными правовыми актами

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов	Первый семестр
Контактная работа (всего)	**34**	**34**
Практические	34	34
Самостоятельная работа (всего)	**38**	**38**
Виды промежуточной аттестации		
Зачет		+
Общая трудоемкость часы	**72**	**72**
Общая трудоемкость зачетные единицы	**2**	**2**

5. Содержание дисциплины

5.1. Содержание дисциплины: Практические (34 ч.)

Первый семестр. (34 ч.)

Тема 1. Сущность и понятие информационной безопасности в системе национальной безопасности. (2 ч.)

Сущность и понятие информационной безопасности в системе национальной безопасности.

Тема 2. Основные понятия и определения в области информационной безопасности (2 ч.)

Основные понятия и определения в области информационной безопасности

Тема 3. Современная доктрина информационной безопасности Российской Федерации. (2 ч.)

Современная доктрина информационной безопасности Российской Федерации.

Тема 4. Цели защиты информации. (2 ч.)

Цели защиты информации.

Тема 5. Объекты информационной безопасности. (2 ч.)

Объекты информационной безопасности.

Тема 6. Государственная тайна и организация ее защиты в Российской Федерации. (2 ч.)

Государственная тайна и организация ее защиты в Российской Федерации.

Тема 7. Коммерческая тайна и организация ее защиты в Российской Федерации. (2 ч.)

Коммерческая тайна и организация ее защиты в Российской Федерации.

Тема 8. Конфиденциальная информация и организация ее защиты в Российской Федерации. (2 ч.)

Конфиденциальная информация и организация ее защиты в Российской Федерации.

Тема 9. Анализ способов нарушения информационной безопасности объектов. (2 ч.)

Анализ способов нарушения информационной безопасности объектов.

Тема 10. Классификация видов, методов и средств защиты информации (2 ч.)

Классификация видов, методов и средств защиты информации

Тема 11. Международные стандарты в области информационной безопасности. (2 ч.)

Международные стандарты в области информационной безопасности.

Тема 12. Национальные стандарты в области информационной безопасности. (2 ч.)

Национальные стандарты в области информационной безопасности.

Тема 13. Анализ типовых моделей угроз информационной безопасности (2 ч.)

Анализ типовых моделей угроз информационной безопасности

Тема 14. Информационная система как регулятор деятельности социальной организации (2 ч.)

Информационная система как регулятор деятельности социальной организации

Тема 15. Информационные войны (2 ч.)

Информационные войны.

Тема 16. Защита общества от деструктивного воздействия информации (2 ч.)

Защита общества от деструктивного воздействия информации.

Тема 17. Психологическое воздействие информации на индивидуальное и массовое сознание. (2 ч.)

Психологическое воздействие информации на индивидуальное и массовое сознание.

6. Виды самостоятельной работы студентов по дисциплине

Первый семестр (38 ч.)

Вид СРС: Подготовка рефератов (19 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. Инструменты деструктивного воздействия на индивидуальное и массовое сознание с помощью информационно-коммуникационных технологий
2. Методы информационно-психологического воздействия в информационно-коммуникационном пространстве.
3. Технология ведения информационной войны.

Вид СРС: Подготовка презентации на заданную тему (19 ч.)

Тематика заданий СРС:

Мультимедийная (электронная/учебная) презентация - это логически связанная последовательность слайдов, объединенных одной тематикой и общими принципами оформления. Мультимедийная презентация представляет сочетание компьютерной анимации, графики, видео, музыки и звукового ряда, которые организованы в единую среду. Чаще всего демонстрация презентации проецируется на большом экране, реже - раздается собравшимся как печатный материал.
Алгоритм самостоятельной работы по подготовке презентации на заданную тему:
1) Ознакомьтесь е предлагаемыми темами презентаций.
2) Ознакомьтесь со списком рекомендуемой литературы и источников и подготовьте их для работы.
3) Повторите лекционный материал по теме презентации (при наличии).
4) Изучите материал, касающийся темы презентации не менее чем по двум-трём рекомендованным источникам.
5) Составьте план-сценарий презентации, запишите его.
6) Проработайте найденный материал, выбирая только то, что раскрывает пункты плана презентации.
7) Составьте, наберите на компьютере и распечатайте текст своего устного выступления. При защите презентации он и будет являться сценарием презентации.
8) Продумайте дизайн презентации.
9) Подготовьте медиафрагменты (аудио-, видеоматериалы, текст и т.п.)
10) Оформите презентацию в соответствии с рекомендациями. Обязательно учтите возможные типичные ошибки и постарайтесь избежать их при создании своей презентации. Внимательно проверьте текст на отсутствие ошибок и опечаток.
11) Проверьте на работоспособность все элементы презентации.
12) Прочтите текст своего выступления медленно вслух, стараясь запомнить информацию.
13) Восстановите последовательность изложения текста сообщения, пересказав его устно.
14) Еще раз устно проговорите своё выступление в соответствии с планом, теперь уже сопровождая своё выступление демонстрацией слайдов па компьютере, делая в тексте пометки в тех местах, где нужна смена слайда.
15) Будьте готовы ответить на вопросы аудитории по теме Вашего сообщения.
К критериям оценки самостоятельной работы по подготовке презентации относятся:
Критерии оценки содержания презентации:
- соответствие материала презентации заданной теме;
- грамотное использование терминологии;
- обоснованное применение эффектов визуализации и анимации;
- общая грамотность;
- логичность изложения материала, доказательность, аргументированность.
Критерии оценки оформления презентации:
- творческий подход к оформлению презентации;
- прослеживается обоснованная последовательность слайдов и информации на слайдах;
- необходимое и достаточное количество фото- и видеоматериалов, учет особенностей восприятия графической (иллюстративной) информации, корректное сочетание фона и

графики;
- дизайн презентации не противоречит ее содержанию;
- грамотное соотнесение устного выступления и компьютерного сопровождения, общее впечатление от мультимедийной презентации.

Темы презентаций:
1. Защита от деструктивного воздействия информации.
2. Примеры ведения информационных войн.
3. Понятие «информационно-психологическое воздействие».

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
	Зачет	
Повышенный	зачтено	91 и более
Базовый	зачтено	71 – 90
Пороговый	зачтено	60 – 70
Ниже порогового	не зачтено	Ниже 60

Критерии оценки знаний студентов по дисциплине

Оценка	Показатели

Зачтено	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.
Не зачтено	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-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства

Студент должен знать:

сущность и понятие информации, информационной безопасности, их роль в современном обществе, значение для обеспечения объективных потребностей личности общества и государства; психологические аспекты информационной безопасности в современном обществе; угрозы и источники угроз информационной
безопасности современного общества; основные методы обеспечения информационной безопасности оперировать базовой терминологией в области информационной безопасности личности, общества и государства, гуманитарных аспектов информационной безопасности, место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России; источники и классификацию угроз информационной безопасности; основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации

Вопросы, задания:

1. Коммерческая тайна и организация ее защиты в Российской Федерации.
2. Конфиденциальная информация и организация ее защиты в Российской Федерации.
3. нализ способов нарушения информационной безопасности объектов

Студент должен уметь:

оперировать базовой терминологией в области информационных технологий, информационной безопасности личности, общества и государства, гуманитарных аспектов информационной безопасности.

Задания:

1. Определять информацию относящуюся к коммерческой тайне.
2. Определять информацию относящуюся к персональным данным.
3. Методы защиты информационной безопасности объектов.

Студент должен владеть навыками:

основными информационными технологиями, базовыми методами выявления и классификации угроз информационной безопасности современного общества, основными подходами к противодействию угроз информационной безопасности

Задания:

1. Определение особенностей хранения информации в разных файловых системах.
2. Восстановление удаленных данных со съемного носителя файловой системы NTFS.
3. Восстановление удаленных данных со съемного носителя файловой системы FAT.

- ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

Студент должен знать:

основные нормативные правовые акты в области информационной безопасности и защиты информации, нормативные и методические документы Федеральной службы безопасности по техническому и экспортному контролю в данной области

Вопросы, задания:

1. Международные стандарты в области информационной безопасности
2. Национальные стандарты в области информационной безопасности
3. Классификация видов, методов и средств защиты информации

Студент должен уметь:

применять нормативные правовые акты в своей профессиональной деятельности

Задания:

1. Сравнение российских и зарубежных стандартов в области ИБ
2. Сравнение методов защиты информации
3. Определение эффективности применяемых методов защиты

Студент должен владеть навыками:

навыками работы с нормативными правовыми актами

Задания:

1. Защита компьютерной информации на логическом уровне
2. Определять методы защиты государственной тайны
3. Различие субъектов и объектов ИБ

8.3. Вопросы промежуточной аттестации

Первый семестр (Зачет)

1. Понятие угрозы информационной безопасности.
2. Виды угроз информационной безопасности РФ.
3. Основные внешние источники угроз информационной безопасности РФ.
4. Основные внутренние источники угроз информационной безопасности РФ.
5. Методы обеспечения информационной безопасности РФ.

6. Ограничение доступа к информации.

7. Виды уязвимости информации.

8. Состояние информационной безопасности РФ и основные задачи по ее обеспечению.

9. Принципы обеспечения информационной безопасности.

10. Особенности обеспечения информационной безопасности в различных сферах общественной жизни.

11. Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации

12. Ограничение доступа к информации.

13. Понятие уязвимости информации.

14. Виды уязвимости информации.

15. Понятие "утечка информации".

16. Соотношение форм и видов уязвимости информации

17. Основные функции системы обеспечения информационной безопасности РФ.

18. Категории информации в зависимости от порядка ее предоставления или распространения.

19. Специфика объектов информационной защиты

20. Значение защиты информации для субъектов информационных отношений государства, общества, личности.

21. Значение защиты информации в политической, военной, экономической и других областях деятельности.

22. Информация ограниченного доступа.

23. Сведения конфиденциального характера.

24. Формы представления конфиденциальной информации.

25. Основные средства защиты информации.

26. Основные методы защиты информации.

27. Требования к системе защиты информации.

28. Понятие государственной тайны.

29. В каких сферах деятельности РФ предусмотрено отнесение сведений к государственной тайне?

30. Основные понятия (категории) в области государственной тайны (допуск к государственной тайне, гриф секретности).

31. Что не подлежит отнесению к государственной тайне и засекречиванию?

32. Принципы отнесения сведений к государственной тайне и засекречиванию.

33. Основные степени секретности сведений, составляющих государственную тайну

34. Принципы отнесения сведений к коммерческой тайне.

35. Понятие коммерческой тайны.

36. Сведения, которые не могут составлять коммерческую тайну.

37. Основные понятия, относящиеся к коммерческой тайне.

38. Последствия разглашения сведений, составляющих коммерческую тайну.

39. Перечень сведений, составляющих коммерческую тайну фирмы.

40. Области применения организационных, криптографических и инженерно-технических методов защиты информации.

41. Понятие и классификация средств защиты информации.

42. Назначение программных, криптографических и технических средств защиты.

43. Характеристика и классификация стандартов в области информационной безопасности.

44. Основные международные и российские стандарты в области информационной безопасности.

45. Понятие персональных данных.

46. Угрозы информационной безопасности персональных данных (источники и характеристика угроз).

47. Права субъекта персональных данных.

48. Доктрина информационной безопасности РФ (в части защиты общества от деструктивного воздействия информации).

49. Понятие «информационная война».

50. Информационные войны в информационно-коммуникационном пространстве.

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

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

Методика формирования результирующей оценки:

Первый семестр

1. Контрольная работа - от 0 до 35 баллов
2. Устный опрос, собеседование - от 0 до 30 баллов
3. Письменные задания или лабораторные работы - от 0 до 35 баллов
4. Зачет - 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. Бабаш, А. В. Информационная безопасность и защита информации [Электронный ресурс]: учебное - Издание 3-е изд - Москва:РИОР : ИНФРА-М, 2016. - 322 с. - Режим доступа: http://znanium.com/go.php?id=495249

2. Щеглов А.Ю., Щеглов К.А. Защита информации: основы теории [Электронный ресурс]: - Бакалавр и магистр. Академический курс, 2018. - 309 с. - Режим доступа: http://www.biblio-online.ru/book/9CD7BE3A-F9DC-4F6D-8EC6-6A90CB9A4E0E

9.2 Дополнительная литература

1. Внуков А.А. Защита информации [Электронный ресурс]: - Издание испр. и доп а2-е изд - Бакалавр и магистр. Академический курс, 2018. - 261 с. - Режим доступа: http://www.biblio-online.ru/book/73BEF88E-FC6D-494A-821C-D213E1A984E1

2. Тараскин, М. М. Комплексная защита информации в организации [Электронный ресурс]: научное - Русайнс, 2017. - 353 с. - Режим доступа: http://www.book.ru/book/922538

3. Щеглов А.Ю., Щеглов К.А. Защита информации: основы теории [Электронный ресурс]: - Бакалавр и магистр. Академический курс, 2018. - 309 с. - Режим доступа: http://www.biblio-online.ru/book/9CD7BE3A-F9DC-4F6D-8EC6-6A90CB9A4E0E

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://lib.volsu.ru - Электронная библиотека Волгоградского государственного университета

2. http://fstec.ru - Официальный сайт Федеральной службы по техническому и экспортному контролю

3. http://ibooks.ru/ - Электронная библиотечная система учебной и научной литературы

4. http://new.volsu.ru/umnik - Образовательный портал Волгоградского государственного университета «УМНИК»

5. https://e.lanbook.com/ - Электронно-библиотечная система

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)

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

Учебные аудитории для проведения практических работ представляют собой компьютерные классы или лаборатории, оснащенные лабораторным оборудованием, в зависимости от степени сложности.
Специализированная мебель:
парта со скамьей- 20 шт.
учебные места - 40 шт.
рабочее место преподавателя (парта со скамьей) – 1 шт.
Демонстрационное оборудование:
1. Доска (меловая)
2. Проектор BenQ MX 505
3. Экран для проектора
Технические средства обучения:
1. Ноутбук 15,6” ASUS P53S/P53SJ, Intel Core i5

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС ВолГУ.