

МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

декан факультета прикладной
математики, информатики
и механики



_____ А.И. Шашкин
подпись, расшифровка подписи

23.05.2020

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.Б.51.10 Современные технологии защиты информации

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

математические методы защиты информации

3. Квалификация (степень) выпускника:

Специалист по защите информации

4. Форма обучения:

очная

5. Кафедра, отвечающая за реализацию дисциплины:

ERP-систем и бизнес-процессов

6. Составители программы:

Крыжановская Юлиана Александровна, старший преподаватель кафедры ERP-систем и бизнес-процессов

7. Рекомендована:

Научно-методическим советом факультета прикладной математики, информатики и механики
23.05.2020 г., протокол № 9

отметки о продлении вносятся вручную)

8. Учебный год: 2024/2025

Семестр(ы): 9

9.Цели и задачи учебной дисциплины: овладение математическим и алгоритмическим аппаратом, используемым при проектировании и реализации средств защиты информации в сетях и системах

10. Место учебной дисциплины в структуре ООП: Дисциплина «Современные технологии защиты информации» входит в базовую часть учебного плана, является дисциплиной специализации и изучается в 9 семестре.

№ п/п	Наименование дисциплин учебного плана, с которым организована взаимосвязь дисциплины рабочей программы
1	Б1.Б.27 Информатика
2	Б1.Б.31 Сети и системы передачи информации
3	Б1.Б.37 Основы информационной безопасности
5	Б1.Б.38 Модели безопасности компьютерных систем
6	Б1.Б.43 Криптографические протоколы
7	Б1.Б.44 Криптографические методы защиты информации
8	Б1.Б.48 Установка и настройка ПО
9	Б1.Б.51.11 Корпоративные информационные системы
10	Б1.Б.51.04 Криптографические стандарты

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Компетенция		Планируемые результаты обучения
Код	Название	
ПСК-2.1	способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации	Знание применяемых в настоящий момент технологий защиты данных Умение применять технологии защиты информации. Владение навыками построения и реализации алгоритмов защиты информации.

12. Объем дисциплины в зачетных единицах/час. (в соответствии с учебным планом) — 4/144.

Форма промежуточной аттестации (зачет/экзамен) зачет с оценкой, курсовая работа.

13. Виды учебной работы

Вид учебной работы		Трудоемкость		
		Всего	По семестрам	
			9 семестр	
Аудиторные занятия		50	50	
в том числе:	лекции	16	16	
	практические	0	0	
	лабораторные	34	34	
Самостоятельная работа		94	94	
Форма промежуточной аттестации (зачет – 0 час. / экзамен – час.)			ЗаО, КР	
Итого:			144	

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
		1. Лекции

1.1	Общие сведения теории информационной безопасности.	Информация как предмет защиты. Угрозы в информационной среде.
1.2	Методы и средства защиты информации.	Методы защиты. Юридические методы защиты. Формальные и неформальные средства защиты. Физические и аппаратные средства защиты. Криптографические средства защиты. Идентификация и аутентификация. Хэширование. Цифровая подпись.
1.3	Технологии защиты информации.	Технология RAID и системы надежного хранения данных. Защита от несанкционированного доступа и копирования. Системы разделения доступа. Аудит. Защита от вредоносного ПО. Системы обнаружения вторжений. Защита информации в сетях. Межсетевые экраны. Технология виртуализации и ее применение в сфере защиты информации.
2. Практические занятия		
3. Лабораторные работы		
3.1	Лабораторная работа №1. Введение в математические проблемы криптографии. Основы теории чисел.	<i>Теоретические сведения</i> 1. Информация как предмет защиты. 2. Угрозы в информационной среде. <i>Практическая часть</i> 1. Осуществить поиск и сбор данных об одном из типов угроз информационной безопасности.
3.2	Лабораторная работа №2. Средства защиты информации	<i>Теоретические сведения</i> 1. Методы защиты. 2. Юридические методы защиты. 3. Формальные и неформальные средства защиты. 4. Физические и аппаратные средства защиты. <i>Практическая часть</i> 1. Выполнить обзор по заданному виду средств защиты.
3.3	Лабораторная работа №3. Криптографические средства защиты.	<i>Теоретические сведения</i> 1. Криптографические средства защиты. 2. Идентификация и аутентификация. 3. Протоколы аутентификации. 4. Хэширование. 5. Цифровая подпись. <i>Практическая часть</i> 1. Программно реализовать указанный алгоритм шифрования. 2. Программно реализовать парольную аутентификацию с указанным типом усложнения алгоритма. 3. Программно реализовать указанный алгоритм хэширования. 4. Программно реализовать указанный алгоритм цифровой подписи.
3.4	Лабораторная работа №4. Технология RAID и системы надежного хранения данных.	<i>Теоретические сведения</i> 1. Технология RAID 2. Системы хранения данных <i>Практическая часть</i> 1. Реализовать построение RAID-массива для ОС Windows или Linux.
3.5	Лабораторная работа №5. Системы разделения доступа. Аудит.	<i>Теоретические сведения</i> 1. Системы разделения доступа. 2. Политика безопасности 3. Аудит. <i>Практическая часть</i> 1. Реализовать (в упрощенном виде) один из вариантов политики безопасности.
3.6	Лабораторная работа №6. Защита от вредоносного ПО. Системы обнаружения вторжений.	<i>Теоретические сведения</i> 1. Защита от вредоносного ПО. 2. Антивирусы. 3. Системы обнаружения вторжений. <i>Практическая часть</i> 1. Осуществить поиск и сбор данных о разрушающих программных средствах указанного типа. 2. Проанализировать работу антивирусного ПО. 3. Проанализировать способы обнаружения атак.

3.7	Лабораторная работа №7. Защита информации в сетях. Межсетевые экраны.	<i>Теоретические сведения</i> 1. Основные направления защиты сети. 2. Задачи управления безопасностью сети. 3. Межсетевые экраны. 4. Виртуальные частные сети. <i>Практическая часть</i> 1. Определить, какие угрозы могут реализоваться в используемой сети и что можно им противопоставить.
3.8	Лабораторная работа №8. Технология виртуализации и ее применение в сфере защиты информации.	<i>Теоретические сведения</i> 1. Технология виртуализации. 2. Типы виртуализации. 3. Применение виртуализации для решения задач по защите информации. <i>Практическая часть</i> 1. Осуществить поиск и сбор информации о заданном типе виртуализации и построенных на его основе средствах защиты.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Общие сведения теории информационной безопасности.	2	0	2	4	8
2	Методы и средства защиты информации.	7	0	20	50	77
3	Технологии защиты информации.	7	0	12	40	59
	Итого:	16	0	34	94	144

14. Методические указания для обучающихся по освоению дисциплины

Изучение теоретического материала, представленного в лекциях, основной и дополнительной рекомендуемой литературе, систематическая подготовка к лабораторным занятиям, к контрольной работе, итоговое повторение теоретического материала к зачету. Подготовка, написание и защита курсовой работы.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины (список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)

а) основная литература:

№ п/п	Источник
1	Дайлип Н. Системы хранения данных в Microsoft Windows / Н. Дайлип. – СПб.: Вильямс, 2004. - 421 с.
2	Программирование алгоритмов защиты информации : учебное пособие / А.В. Домашев [и др.]. – М. : Нолидж, 2000. – 288с.
3	Гулятьев А.К. Виртуальные машины : несколько компьютеров в одном / А. К. Гулятьев. СПб. : Питер. – 2006. 224с.
4	Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства : учебное пособие / В. Ф. Шаньгин. – М. : ДМК Пресс, 2008. – 542 с.

б) дополнительная литература:

№ п/п	Источник
1	Воронков Б.Н. Нормативно-правовые и организационные методы обеспечения информационной безопасности при разработке устройств, использующих средства криптозащиты : учебное пособие / Б.Н. Воронков, В. А. Кузнецов. – Воронеж : ИПЦ ВГУ, 2011. – 136 с.
2	Воронков Б.Н. Методическое пособие по разработке средств защиты информации в вычислительных сетях / Б.Н. Воронков, В. И. Тупота. – Воронеж : ВГУ, 2000. – 256 с.
2	Криптографические методы защиты информации : учебно-методическое пособие / сост.: Б. Н. Воронков, Ю. А. Крыжановская. — Воронеж : Издательский дом ВГУ, 2018. — 113 с.

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)*:

№ п/п	Ресурс
1.	https://e.lanbook.com/ - ЭБС «Лань»

* Вначале указываются ЭБС, с которыми имеются договоры у ВГУ, затем открытые электронно-образовательные ресурсы

16. Перечень учебно-методического обеспечения для самостоятельной работы (учебно-методические рекомендации, пособия, задачки, методические указания по выполнению практических (контрольных) работ и др.)

В качестве формы организации самостоятельной работы применяются методические указания для самостоятельного освоения рассматриваемых технологий. Также предусмотрено получение консультаций по вопросам изучаемой дисциплины, изучение теоретического материала, представленного в лекциях, основной и дополнительной рекомендуемой литературе, выполнение индивидуальных и групповых заданий лабораторных работ, итоговое повторение теоретического материала. Также к СРС относится подготовка к контрольной работе, написание, оформление и защита курсовой работы.

17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)

Windows7, Microsoft Visual Studio Community, браузер, выход в Internet. Мультимедийные лекционные демонстрации. Презентации на базе конспекта лекций.

18. Материально-техническое обеспечение дисциплины:

Лекционная аудитория оснащена специальной мебелью современным компьютером с подключенным к нему проектором и настенным экраном. Лаборатория оснащена современными компьютерами с установленным программным обеспечением, позволяющим выполнять изучение, освоение рассматриваемых технологий, реализовывать различные алгоритмы и подходы к защите данных.

19. Фонд оценочных средств:

19.1. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции (или ее части)	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	ФОС* (средства оценивания)
ПСК-2.1. способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации	Знать применяемые в настоящий момент технологий защиты данных	Раздел 1. Общие сведения теории информационной безопасности. Раздел 2. Методы и средства защиты информации. Раздел 3. Технологии защиты информации.	Устный опрос, лабораторные работы. Контрольная работа. Курсовая работа.
	Уметь применять технологии защиты информации.	Раздел 1. Общие сведения теории информационной безопасности. Раздел 2. Методы и средства защиты информации. Раздел 3. Технологии защиты информации.	Устный опрос, лабораторные работы. Контрольная работа. Курсовая работа.
	Владеть навыками построения и реализации алгоритмов защиты информации	Раздел 1. Общие сведения теории информационной безопасности. Раздел 2. Методы и средства защиты информации. Раздел 3. Технологии защиты информации.	Устный опрос, лабораторные работы. Контрольная работа. Курсовая работа.
Промежуточная аттестация			КИМ

* В графе «ФОС» в обязательном порядке перечисляются оценочные средства текущей и промежуточной аттестаций.

19.2 Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Промежуточная аттестация включает в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и результаты выполнения лабораторных работ, позволяющие оценить степень сформированности умений и навыков.

Для оценивания результатов обучения на зачете используется приведенная ниже шкала.

Соотношение показателей, критериев и шкалы оценивания результатов обучения.

Компетенция	Показатель сформированности компетенции	Шкала и критерии оценивания уровня освоения компетенции			
		5	4	3	2
ПК-2.1. Способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации.	Знает: – применяемые в настоящий момент технологии защиты данных.	Сформированные знания	Сформированные знания, но содержащие отдельные пробелы	Неполные знания	Фрагментарные знания или их отсутствие
	Умеет: – применять технологии защиты информации.	Сформированные умения	Успешные умения, но содержащие отдельные пробелы	Успешные, но не системные умения	Фрагментарные умения или отсутствие умений
	Владеет: – навыками построения и реализации алгоритмов защиты информации	Сформированные умения	Успешные умения, но содержащие отдельные пробелы	Успешные, но не системные умения	Фрагментарные умения или отсутствие умений

19.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

19.3.1 Примерный перечень вопросов к зачету:

1. Правовая защита информации. Структура законодательства.
2. Государственная, служебная, коммерческая тайна (законодательство).
3. Угрозы ИБ.
4. Формальные и неформальные средства защиты.
5. Физические и аппаратные средства защиты.
6. Системы разделения доступа.
7. Аудит.
8. Задачи криптографии.
9. Электронная цифровая подпись.
10. Персональные данные.
11. Технология RAID. Способы реализации.
12. Технология RAID. Уровень 0.
13. Технология RAID. Уровень 1.
14. Технология RAID. Уровень 2,3.
15. Технология RAID. Уровень 4,5.
16. Технология RAID. Уровень 6,7.
17. Технология RAID. Комбинирование уровней.
18. СХД: определения, решаемые задачи.
19. Представление о дисковом пространстве как об одном общем пуле хранилищ.
20. Компоненты СХД.
21. Архитектура DAS.
22. Архитектура NAS.
23. Архитектура SAN.
24. Протокол Fibre Channel.

25. Протокол iSCSI.
26. Протокол SAS.
27. СХД с расширяющейся архитектурой.
28. Технологии виртуализации. .
29. Виртуальные машины. Виртуальная инфраструктура.
30. Виртуализация платформ. Типы.
31. Виртуализация ресурсов.
32. Области применения виртуализации.
33. Применение виртуализации в сфере безопасности.
34. Защита от вредоносного ПО.
35. Защита информации в сетях.
36. Межсетевые экраны.
37. Технология виртуализации и ее применение в сфере защиты информации.
38. Защита от НСД.
39. Анализ регистрационной информации.
40. Системы контроля и управления доступом.
41. Идентификация и аутентификация.
42. Изоляция (защита периметра) компьютерных сетей.
43. Виртуальные частные сети.
44. Криптографическое закрытие данных.
45. Резервное копирование.
46. Обнаружение атак.
47. Утечка информации.
48. НСК: определения, типы защитных мер.
49. Требования к системам защиты от копирования.

19.3.2 Перечень практических заданий

Не предусмотрены

19.3.3 Тестовые задания

Не предусмотрены

19.3.4 Примерный перечень заданий для контрольной работы

Вариант 1.

1. Цифровая подпись на основе алгоритма DES.
2. Хэширование SHA-2.
3. Виртуализация платформ
4. Правовые аспекты защиты данных
5. Firewall
6. RAID 2, 3.
7. Защита от копирования.
8. Типы РПС

Вариант 2.

1. Цифровая подпись на основе алгоритма DES.
2. Российский стандарт хэширования
3. Sand box.
4. Закон о государственной тайне.
5. Задачи управления безопасностью сети.
6. Программно-аппаратная реализация RAID.
7. Резервное копирование.
8. Антивирусное ПО.

19.3.5 Примерные темы курсовых работ

1. Система изучения криптографических алгоритмов.
2. Повышение надежности передачи информации по сети в условиях помех со стороны нарушителя.

3. Разработка системы работы с данными медицинского назначения.
4. Система разделения доступа по ролям.
5. Реализация модели политики доменов и типов.
6. Исследование атак типа РНР-инъекций и методов их предотвращения.
7. Реализация ЭЦП средствами прикладных API операционных систем.
8. Разработка системы распознавания реальных пользователей при аутентификации (CAPTCHA).
9. Исследование методов стеганографии, программная реализация одного из методов.
10. Разработка системы сертификации открытых ключей.
11. Исследование методов защиты программ от несанкционированного запуска.
12. Исследование программных интерфейсов управления доступом к ресурсам ОС. Программная реализация возможности изменения прав доступа произвольной учетной записи или группы к ресурсам системы.
13. Реализация системы аутентификации на основе клавиатурного почерка.
14. Реализация системы распределенной аутентификации типа «запрос-ответ».
15. Исследование методов защиты программ от отладчиков. Программная реализация одного из методов.
16. Реализация асимметричной криптографии средствами прикладных API.
17. Исследование методов обфускации исходного кода.
18. Разработка системы моделирования мандатного доступа к ресурсам ОС.
19. Исследование методов генерации криптостойких случайных чисел с проверкой по тестам FIPS-140.
20. Реализовать один из методов генерации сверхбольших простых чисел с вероятностной проверкой на простоту.
21. Осуществить формирование и верификацию ЭЦП для выбранного файла по ГОСТ 34.10-2012.

Тема курсовой работы может быть предложена обучающимся, должна быть согласована с руководителем и должна соответствовать содержанию (направлению) дисциплины

Критерии оценивания курсовой работы

Для оценивания результатов обучения при выполнении студентом курсовой работы используются следующие показатели:

Знание применяемых в настоящий момент современных технологий защиты данных

Умение применять технологии защиты информации.

Владение навыками построения и реализации алгоритмов защиты информации

Для оценивания результатов выполнения курсовой работы используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Соотношение показателей, критериев и шкалы оценивания результатов выполнения курсовой работы:

Показатель оценивания компетенции	Критерии оценивания компетенций	Шкала оценок
Знание применяемых в настоящий момент технологий защиты данных Умение применять технологии защиты информации. Владение навыками построения и реализации алгоритмов защиты информации	В ходе выполнения и защиты курсовой работы обучающийся продемонстрировал отличное знание применяемых в настоящий момент технологий защиты данных, умение применять технологии защиты информации, владение навыками построения и реализации алгоритмов защиты информации. Привел логичное, доказательное решение некоторой конкретной задачи, проанализировал полученные в ходе ее решения результаты. Курсовая работа оформлена в соответствии с требованиями по оформлению. В соответствии с методикой оценивания оценка за выполнение курсовой работы – 5 баллов.	Отлично
Знание применяемых в настоящий момент	В ходе выполнения и защиты курсовой	Хорошо

технологий защиты данных Умение применять технологии защиты информации. Владение навыками построения и реализации алгоритмов защиты информации	работы обучающийся продемонстрировал знание применяемых в настоящий момент технологий защиты данных , умение применять технологии защиты информации, владение навыками построения и реализации алгоритмов защиты информации, Привел решение некоторой конкретной задачи, проанализировал полученные в ходе ее решения результаты. Курсовая работа оформлена в соответствии с требованиями по оформлению. В соответствии с методикой оценивания оценка за выполнение курсовой работы . – 4 балла.	
Знание применяемых в настоящий момент технологий защиты данных Умение применять технологии защиты информации. Владение навыками построения и реализации алгоритмов защиты информации	В ходе выполнения и защиты курсовой работы обучающийся показал знание применяемых в настоящий момент технологий защиты данных, умение применять технологии защиты информации. Курсовая работа оформлена с замечаниями. В соответствии с методикой оценивания оценка за выполнение курсовой работы – 3 балла.	Удовлетворительно
Знание применяемых в настоящий момент технологий защиты данных Умение применять технологии защиты информации. Владение навыками построения и реализации алгоритмов защиты информации	Обучающийся не справился с выполнением курсовой работы, результаты работы не соответствуют указанным выше критериям. Курсовая работа не оформлена в соответствии с требованиями. В соответствии с методикой оценивания оценка за выполнение курсовой работы составляет менее 3 баллов.	Неудовлетворительно

В ходе выполнения курсовой работы обучающийся демонстрирует знания, умения и навыки, полученные в результате освоения дисциплины.

Теоретический блок курсовой работы:

2 балла – теоретический материал соответствует теме курсовой работы, в полном объеме отражает ее (приведены необходимые доказательства);

1 балл - теоретический материал соответствует теме курсовой работы, кратко отражает ее (отсутствуют необходимые доказательства);

0 баллов - теоретический материал не соответствует теме курсовой работы.

Практический блок курсовой работы:

2 балла – приведенная задача отражает применение теоретического материала, ее решение верно и логично описано;

1 балл – приведенная задача отражает применение теоретического материала, но ее решение кратко или содержит ошибки;

0 баллов – задача отсутствует, или приведенная задача не является практическим применением теоретического материала курсовой работы.

Защита курсовой работы:

1 балл – в процессе подготовки к выполнению курсовой работы и ее написания обучающийся продемонстрировал самостоятельность, самоорганизованность, инициативность, ответственность; во время защиты курсовой работы студент показал знание материала курсовой работы, ответил на дополнительные вопросы по теме работы;

0 баллов – во время подготовки к выполнению курсовой работы и ее написания обучающийся проявил неорганизованность, безынициативность, безответственность; во время защиты курсовой работы студент неуверенно отвечал на вопросы по теме работы, допускал ошибки.

Таким образом, максимальное количество баллов, которое обучающий может получить за курсовую работу, равно 5. Критерии выставления оценки («отлично», «хорошо», «удовлетворительно», «неудовлетворительно») за выполнение курсовой работы приведены выше.

Курсовая работа имеет следующую структуру:

- титульный лист;
- содержание;
- текст работы – содержательная часть курсовой работы;
- список литературы;
- приложения (при необходимости).

Содержательная часть курсовой работы представляет собой 2 блока: теоретический (теоретический материал по теме курсовой работы) и практический (применение теории к решению конкретной задачи). В завершении данной части стоит подвести итог выполненной работы (что было изучено и какой результат получен).

Текст работы располагается на одной стороне листа белой бумаги формата А4 по ГОСТ 2.30168 (размер 210 × 297 мм). допускается представлять иллюстрации и таблицы на листах формата не более 420 × 594 мм, должны соблюдаться следующие размеры полей:

- левое - не менее 30 мм;
- правое - не менее 10 мм;
- верхнее - не менее 15 мм;
- нижнее - не менее 20 мм.

Текст работы может быть набран в текстовом редакторе Microsoft Word шрифтом Times New Roman (14 пунктов) через полтора интервала. Абзацный отступ равен 10-17 мм.

На страницах номер проставляют, как правило, сверху по центру. На титульном листе номер не ставится, но включается в общую нумерацию работы. Объем работы составляет 10-20 листов. Количество используемых библиографических источников – не менее 5.

Скрепленная и оформленная надлежащим образом курсовая работа предоставляется обучающимся на проверку преподавателю. В срок, установленный календарным учебным графиком, через 1-3 рабочих дня после предоставления обучающимся работы преподавателю на проверку, происходит защита курсовой работы, в ходе которой обучающийся должен показать уверенное знание материала работы.

19.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах: устного опроса; лабораторных работ; контрольной работы. Критерии оценивания приведены выше.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Контрольно-измерительные материалы промежуточной аттестации включают в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и практическое задание, позволяющее оценить степень сформированности умений и навыков работы с технологиями защиты информации.

При оценивании используются качественные шкалы оценок. Критерии оценивания приведены выше.