МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный университет»

«Утверждаю»
Заведующий кафедрой ТО и ЗИ

«05» июля 2018 г.  А.А. Сирота

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.ДВ.2.1 Диагностика и защита от вредоносных программ

1.Шифр и наименование направления подготовки/специальности:
09.04.02 Информационные системы и технологии

2. Профиль подготовки/специализации: безопасность информационных систем

3. Квалификация (степень) выпускника: магистр

4. Форма образования: очная

5. Кафедра, отвечающая за реализацию дисциплины:
Кафедра технологий обработки и защиты информации

6. Составители программы:
Вялых Сергей Ариевич, к.т.н., доцент

7. **Рекомендована:**
Научно-методическим советом ФКН, протокол № 6 от 25.06.2018 г.

(отметки о продлении вносятся вручную)

8. Учебный год: 2019-2020 **Семестр(ы):** 4

9. Цели и задачи учебной дисциплины: Целью курса «Диагностика и защита от вредоносных программ» является освоение студентами основных положений теории защиты информации от вредоносных программ и методологии оценки угроз безопасности информации, характерных для современных информационных технологий. Должно быть сформировано представления об основных видах вредоносных программ, их потенциальных возможностях и об угрозах безопасности информации, которые могут быть ими реализованы в компьютерных системах.

Основные задачи дисциплины:

- освоение студентами положений и требований, современных нормативно-методических документов, регламентирующих меры защиты от вредоносных программ;
- формирование представления об основных видах вредоносных программ, их потенциальных возможностях и об угрозах безопасности информации, которые могут быть ими реализованы в компьютерных системах;
- изучение основных положений теории защиты информации от вредоносных программ;
- формирование представления о приемах и методах исследования возможностей вредоносных программ;
- овладение практическими навыками защиты информационных систем от вредоносных программ.

10. Место учебной дисциплины в структуре ООП: Блок Б1.В дисциплины относится к вариативной части профессионального цикла (дисциплина по выбору).

Для успешного освоения дисциплины необходимы входные знания в области основ информационной безопасности, организационного и правового обеспечения информационной безопасности, архитектуры информационных систем, навыки программирования.

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	
ПК-8	Умение проводить разработку и исследование теоретических и экспериментальных моделей объектов профессиональной деятельности в областях: машиностроение, приборостроение, наука, техника, образование, медицина, административное управление, юриспруденция	**знать:** положения и требования, современных нормативно-методических документов, регламентирующих меры защиты от вредоносных программ; **уметь:** анализировать и обобщать материалы научно-технической литературы, нормативных и методических материалов по вопросам защиты информации от вредоносных программ; **владеть:** практическими навыками использования современных антивирусных средств защиты информации.
ПК-11	Умение осуществлять постановку и проведение экспериментов по заданной методике и анализ результатов	**знать:** основные положения теории защиты информации от вредоносных программ, методы и возможности обнаружения вредоносных программ; **уметь**: проводить анализ объектов и систем на соответствие требованиям нормативных документов в области защиты от вредоносных программ; **владеть**: практическими навыками формирования требований и контроля выполнения требований и мер по антивирусной защите информации.

12. Объем дисциплины в зачетных единицах/час — 3/108.
Форма промежуточной аттестации: *зачет*.

13. Виды учебной работы:

Вид учебной работы	Трудоемкость			
	Всего	По семестрам		
		№ семестра 4	№ семестра	Итого
Аудиторные занятия	28	28		28
в том числе: лекции	-	-		-
практические	14	14		14
лабораторные	14	14		14
Самостоятельная работа	80	80		80
Форма промежуточной аттестации *(зачет – __ час. / экзамен – 0 час.)*	-	-		-
Итого:	108	108		108

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1. Лекции		
1.1	нет	
2. Практические занятия		
2.1	Виды вредоносных программ	1. Основные виды вредоносных программ и особенности их функционирования. История вопроса. Классификация компьютерных вирусов. Признаки присутствия на компьютере вредоносных программ.
2.2	Исследование возможностей наиболее распространенных антивирусных программ	2. Исследование возможностей наиболее распространенных антивирусных программ. Особенности использования программы обнаружения вредоносных программ AVZ. Скрипты и управление AVZ.
2.3	Теоретические сведения о вредоносных программах	3. Теоретические сведения о компьютерных вирусах. Формальные модели и исследование потенциальных возможностей вредоносных программ. Основные положения теории алгоритмов. Машина Тъюринга. 4. Модели компьютерного вируса, сетевого червя. Оценка потенциальных алгоритмических свойств вредоносных программ. Современные тенденции развития угроз безопасности информации, связанные с применением программного обеспечения.
2.4	Практические методы и приемы исследования вредоносных программ	5. Практические методы и приемы исследования вредоносных программ. Отладчики и дизассемблеры. Основные возможности отладчиков Soft-Ice, IDA, OllyDbg.
2.5	Основные технологии разработки вредоносных программ	6. Архитектура построения современных вычислительных систем с точки зрения возможностей воздействия вредоносных программ. Возможности низкоуровневого воздействия. Современные тенденции развития угроз безопасности информации, связанные с вредоносными программами.
2.6	Типовые способы и средства компьютерной разведки	7. Понятие, основные этапы, типовые способы и средства компьютерной разведки. Современные сканеры уязвимостей информационных систем.
2.7	Основные направления защиты от вредоносных программ	8. Основные направления защиты от вредоносных программ. Средства обнаружения вторжений.
3. Лабораторные работы		
3.1	Виды вредоносных программ	1. Знакомство с первыми компьютерными вирусами. Вирус 1701 (падающие буквы).
3.2	Исследование возможностей наиболее распространенных антивирусных программ	2. Исследование основных возможностей антивирусных программ лаборатории Касперского. 3. Исследование программы обнаружения вредоносных программ AVZ. Скрипты и управление AVZ.
3.3	Теоретические сведения о вредоносных программах	4. Знакомство с полиморфными программными вирусами и генераторами вредоносных программ.
3.4	Практические методы и приемы исследования вредоносных программ	5. Отладчики и дизассемблеры. Основные возможности отладчиков Soft-Ice, IDA, OllyDbg.
3.5	Типовые способы и средства компьютерной разведки	6. Исследование возможностей современных сканеров уязвимостей информационных систем.

		7. Средства тестирования на проникновение.
3.6	Основные направления защиты от вредоносных программ	8. Средства обнаружения вторжений.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)			
		Практические	Лабораторные	Сам. работа	Всего
1	Виды вредоносных программ.	2	2	4	8
2	Исследование возможностей наиболее распространенных антивирусных программ	2	4	20	26
3	Теоретические сведения о вредоносных программах.	2	2	4	8
4	Практические методы и приемы исследования вредоносных программ.	2	2	18	22
5	Основные технологии разработки вредоносных программ	2	-	8	10
6.	Типовые способы и средства компьютерной разведки	2	2	10	14
7	Основные направления защиты от вредоносных программ.	2	2	16	20
	Итого:	14	14	80	108

14. Методические указания для обучающихся по освоению дисциплины

(рекомендации обучающимся по освоению дисциплины: работа с конспектами лекций, презентационным материалом, выполнение практических заданий, тестов, заданий текущей аттестации и т.д.)

1) При изучении дисциплины рекомендуется использовать следующие средства**:**

- рекомендуемую основную и дополнительную литературу;
- методические указания и пособия;
- контрольные задания для закрепления теоретического материала;
- электронные версии учебников и методических указаний для выполнения лабораторно - практических работ (при необходимости материалы рассылаются по электронной почте).

2) Для максимального усвоения дисциплины рекомендуется проведение письменного опроса (тестирование практического использования программных средств) студентов по материалам лабораторных практических работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала. Такой подход позволяет повысить мотивацию студентов при изучении материала.

3) При проведении лабораторных занятий обеспечивается максимальная степень соответствия с материалом занятий и осуществляется экспериментальная проверка методов, алгоритмов и технологий обработки информации, излагаемых в рамках лекций.

4) В ходе самостоятельной работы основное внимание необходимо уделить изучению возможностей антивирусных средств доступных на сайтах http://www.z-oleg.com/ и http://www.kaspersky.ru/.

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	Ховард, Майкл. 19 смертных грехов, угрожающих безопасности программ. Как не допустить типичных ошибок : / М. Ховард, Д. Лебланк, Дж. Виега ; авт. предисл. А. Йоран .— Москва : ДМК Пресс, 2009 .— 287 с. : ил. — .— Загл. и авт. ориг.: 19 deadly sins of soft-ware security / Michael Howard, David Leblanc, John Viega .— ISBN 5-9706-0027-X .— <URL:http://e.lanbook.com/books/element.php?pl1_cid=25&pl1_id=1118>.
2	Касперский, Евгений Валентинович. Компьютерное zловредство / Евгений Касперский .— СПб. [и др.] : Питер, 2007 .— 207 с. : ил. + 1 CD https://lib.vsu.ru/zgate?present+4408+default+2+1+F+1.2.840.10003.5.102+rus

б) дополнительная литература:

№ п/п	Источник
3	Зайцев О.В. Rootkits, SpyWare/AdWare, Keyloggers & BackDoors : Обнаружение и защита / О.В. Зайцев. – СПб.: БХВ-Петербург, 2006. - 304 с.
4	Голуб, Владимир Александрович. Защита от вредоносного программного обеспечения: учебное пособие для вузов / В.А. Голуб; Воронеж. гос. ун-т.— Воронеж: ЛОП ВГУ, 2006 .— 31 с. — Библиогр.: с.30 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/may07045.pdf>.
5	Мельников, Владимир Павлович. Информационная безопасность и защита информации: учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова .— М. : ACADEMIA, 2006 .— 330 с. : ил .— (Высшее профессиональное образование. Информатика и вычислительная техника) .— Библиогр.: с.327-328 .— ISBN 5-7695-2592-4.
6	Пирогов В.Ю. Ассемблер и дизассемблирование / В.Ю. Пирогов. – СПб.: БХВ-Петербург, 2006. - 464 с.
7	Александр Доронин. Бизнес-разведка http://fxt.com.ua/business_literatura/131-aleksandr-doronin-biznes-razvedka.html
8	Вялых А.С. Оценка возможностей атаки на информационную систему / А.С. Вялых, С.А. Вялых // Кибернетика и высокие технологии XXI века : матер. XII международ. науч.-тех. конф., Воронеж, 11-12 мая 2011 г. – Воронеж : ИПЦ ВГУ, 2011. – Т.1. – С. 91-96.

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

№ п/п	Ресурс
9	http://www.z-oleg.com/
10	http://www.kaspersky.ru/
11	Материалы Интернет-Университета Информационных Технологий www.INTUIT.ru
12	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
13	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)
14	ЭБС «Издательства «Лань», Договор №3010-06/71-14 от 25.11.2014, ЭБС «Университетская библиотека online», Договор №3010-06/70-14 от 25.11.14, Национальный цифровой ресурс «РУКОНТ», Договор №ДС-208 от 01.02.2012

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

16. Перечень учебно-методического обеспечения для самостоятельной работы

(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)

№ п/п	Источник
1	Пирогов В.Ю. Ассемблер и дизассемблирование / В.Ю. Пирогов. – СПб. : БХВ-Петербург, 2006. - 464 с.
2	Зайцев О.В. Rootkits, SpyWare/AdWare, Keyloggers & BackDoors : Обнаружение и защита / О.В. Зайцев. – СПб. : БХВ-Петербург, 2006. - 304 с.

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

Для реализации учебного процесса используются:

1) ПО Microsoft в рамках подписок «Imagine»,ежегодные сублицензионные договоры № 56035/BPH3739 и № 56036/BPH3739 от 07.10.2016.

2) Средства виртуализации VMware, образы операционных систем семейства Windows, доступ в Интернет.

3) Тестовые дистрибутивы антивирусных программ и средств анализа уязвимостей.

18. Материально-техническое обеспечение дисциплины:

(при использовании лабораторного оборудования указывать полный перечень, при большом количестве оборудования можно вынести данный раздел в приложение к рабочей программе)

1) Мультимедийная лекционная аудитория (корп.1а, ауд. № 479), ПК-Intel-i3, рабочее место преподавателя: проектор, видеокоммутатор, микрофон, аудиосистема, специализированная мебель: доски меловые 2 шт., столы 60 шт., лавки 30 шт., стулья 64 шт.; доступ к фондам учебно-методической документации и электронным библиотечным системам, выход в Интернет.

2) Компьютерный класс (один из №1-4 корп. 1а, ауд. № 382-385),ПК-Intel-i3 16 шт., специализированная мебель: доска маркерная 1 шт., столы 16 шт., стулья 33 шт.; доступ к фондам учебно-методической документации и электронным изданиям, доступ к электронным библиотечным системам, выход в Интернет.

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)
ПК-8, уметь проводить разработку и исследование теоретических и экспериментальных моделей объектов профессиональной деятельности в областях: машиностроение, приборостроение, наука, техника, образование, медицина, административное управление, юриспруденция	**знать:** положения и требования, современных нормативно-методических документов, регламентирующих меры защиты от вредоносных программ.	Разделы 1-2 Исследование возможностей наиболее распространенных антивирусных программ	Контрольная работа по соответствующим разделам. Лабораторные работы 2-3
	уметь: анализировать и обобщать материалы научно-технической литературы, нормативных и методических материалов по вопросам защиты информации от вредоносных программ.	Разделы 2-4 Исследование возможностей наиболее распространенных антивирусных программ. Теоретические сведения. Практические методы и приемы исследования вредоносных программ.	Контрольная работа по соответствующим разделам. Лабораторные работы 2-4, 8
	владеть: практическими навыками использования современных антивирусных средств защиты информации.	Разделы 2-4 Исследование возможностей наиболее распространенных антивирусных программ. Теоретические сведения. Практические методы и приемы исследования вредоносных	Лабораторные работы 2-5, 8

		программ.	
ПК-11, уметь осуществлять постановку и проведение экспериментов по заданной методике и анализ результатов	**знать:** основные положения теории защиты информации от вредоносных программ, методы и возможности обнаружения вредоносных программ .	Разделы 3-7 Теоретические сведения. Практические методы и приемы исследования вредоносных программ. Сканеры уязвимостей. Средства обнаружения вторжений.	Контрольная работа по соответствующим разделам. Лабораторные работы 5-8.
	уметь: проводить анализ объектов и систем на соответствие требованиям нормативных документов в области защиты от вредоносных программ.	Разделы 2, 5-7 Исследование возможностей наиболее распространенных антивирусных программ. Теоретические сведения. Практические методы и приемы исследования вредоносных программ. Сканеры уязвимостей. Средства обнаружения вторжений.	Контрольная работа по соответствующим разделам. Лабораторные работы 2.
	владеть: практическими навыками формирования требований и контроля выполнения требований и мер по антивирусной защите информации	Разделы 2, 5-7 Исследование возможностей наиболее распространенных антивирусных программ. Теоретические сведения. Практические методы и приемы исследования вредоносных программ. Сканеры уязвимостей. Средства обнаружения вторжений.	Контрольная работа по соответствующим разделам. Лабораторные работы 2,6-8.
Промежуточная аттестация			Комплект 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

Для оценивания результатов обучения на экзамене используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

1) знание теоретических основ учебного материала, основных определений, понятий и используемой терминологии;

2) умение проводить обоснование и представление основных практических результатов с использованием антивирусных средств и средств анализа уязвимостей;

3) умение иллюстрировать ответ примерами, в том числе, собственными, умение выявлять и анализировать основные закономерности, полученные, в том числе, в ходе выполнения лабораторно-практических заданий;

4) умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу;

5) владение навыками программирования и экспериментирования с антивирусными средствами в рамках выполняемых лабораторных заданий;

6) владение навыками проведения компьютерного эксперимента, тестирования антивирусных алгоритмов обработки информации.

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций) на государственном экзамене:

- высокий (углубленный) уровень сформированности компетенций;
- повышенный (продвинутый) уровень сформированности компетенций;
- пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на государственном экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Для оценивания результатов обучения на зачете используется – зачтено, не зачтено по результатам тестирования.

Соотношение показателей, критериев и шкалы оценивания результатов обучения на государственном экзамене представлено в следующей таблице.

Критерии оценивания компетенций и шкала оценок на зачете

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	Неудовлетворительно

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 применяемых оценочных средств

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ - не зачтено
2	Контрольная работа по разделам дисциплины	Теоретические вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной в разделе 19.2
3	Лабораторная работа	Содержит 9 лабораторных задания, предусматривающие разработку, тестирова-	При успешно выполнении работы ставится оценка зачтено и осуществляется допуск к экзамену, в

		ние и эксплуатацию моделей и алгоритмов анализа данных с использованием различных методов обучения.	противном случае ставится оценка не зачтено и обучающийся не допускается к экзамену.
4	КИМ промежуточной аттестации	Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает 2 вопроса для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции.	Шкалы оценивания приведены в разделе 19.2

19.3.2. Примерный перечень вопросов к зачету

№	Содержание
1	Классификация вредоносных программ
2	Признаки присутствия на компьютере вредоносных программ
3	Модель компьютерного вируса
4	Модель сетевого червя
5	Оценка потенциальных алгоритмических свойств вредоносных программ
6	Возможности использования программы обнаружения вредоносных программ AVZ
7	Отладчики и дизассемблеры. Основные возможности отладчика Soft-Ice.
8	Классификация антивирусных программ и их основные возможности
9	Основные возможности и способы компьютерной разведки
10	Возможности сетевых сканеров обнаружения уязвимостей (на примере XSpider).
11	Основные средства и их возможности защиты компьютерной сети
12	Возможности низкоуровневого воздействия вредоносных программ. Программы-шпионы (кейлогеры)
13	Модель угроз безопасности информации. Современные тенденции развития вредоносных программ
14	Программа APS (Anti Port Scanner) и её возможности
15	Современные методики оценки уязвимостей информационных систем
16	Основные возможности антивирусной программы Kaspersky Internet Security
17	Основные возможности антивирусной программы и особенности применения Kaspersky Endpoint Security

19.3.3. Пример задания для выполнения лабораторной работы

Лабораторная работа № 2

«Исследование возможностей наиболее распространенных антивирусных программ. Особенности использования программы обнаружения вредоносных программ AVZ. Скрипты и управление AVZ»

Цель работы:
Исследовать возможности антивирусных средств защиты информации.
Форма контроля: отчёт в электронном виде
Количество отведённых аудиторных часов: 4

Задание:

Получите у преподавателя вариант задания, образ операционной системы и дистрибутив антивирусного средства. Для ответа на поставленные вопросы требуется проинсталлировать антивирусное средство на виртуальную машину. Оценить возможности антивирусного средства. Разработайте скрипт управления антивирусным средством в соответствии с вариантом задания. Составьте отчёт о проделанной работе, в котором отразите следующие пункты:

- ФИО исполнителя и номер группы.
- Название и цель лабораторной работы.
- Номер своего варианта.
- Код, написанный исполнителем.

- Краткие выводы об исследованных возможностях антивирусного средства.

Примеры контрольных вопросов:

1. Какие основные параметры операционной системы может контролировать AVZ.
2. Какие возможности контроля предоставляют скрипты управления антивирусным средством.

Варианты заданий:

1. Разработка скрипта для сканирования сети.
2. Лечение заданных папок по заданному условию.
3. Сканирование и помещение подозрительных файлов на автокарантин.
4. Обновление баз с протоколированием
5. Разработка скрипта удаления троянской программы с известным именем.
6. Разработка скрипта сканирования и отправки результатов по почте.
7 Разработка скрипта контроля целостности заданных файлов.

19.3.4. Пример контрольно-измерительного материала

УТВЕРЖДАЮ
Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота
__.__.2018

Направление подготовки / специальность 10.03.01 Информационная безопасность

Дисциплина Б1.В.ДВ.02.01 Защита от вредоносных программ

Форма обучения Очное

Вид контроля Зачет

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Классификация вредоносных программ.
2. Основные возможности антивирусной программы и особенности применения Kaspersky Endpoint Security.

Преподаватель _____ С.А. Вялых

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 (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы). При оценивании могут использоваться количественные или качественные шкалы оценок.

Промежуточная аттестация может включать в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и/или практическое (ие) задание(я), позволяющее (ие) оценить степень сформированности умений и навыков.

При оценивании используется количественная шкала. Критерии оценивания приведены выше в таблице раздела 19.2.