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

УТВЕРЖДАЮ
Заведующий кафедрой
теории функций и геометрии

_____Е.М. Семенов
11.04.2024 г

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.11 Анализ защищенности информационных систем

1. Код и наименование специальности:
10.05.04 Информационно-аналитические системы безопасности

2. Специализация: Автоматизация информационно-аналитической деятельности

3. Квалификация (степень) выпускника: Специалист по защите информации

4. Форма обучения: Очная

5. Кафедра, отвечающая за реализацию дисциплины:
Кафедра теории функций и геометрии

6. Составители программы:
Шипилова Елена Алексеевна, к.т.н., доцент

7. **Рекомендована:** Научно-методическим Советом математического факультета, протокол № 0500-03 от 28.03.2024 г.

8. Учебный год: 2028/2029 **Семестр(-ы):** 8

9. Цели и задачи учебной дисциплины:

Цели изучения дисциплины:

- изучение основ информационной безопасности и защиты информации; типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду.

Задачи дисциплины:

- изучить основные понятия надежности информационных систем; количественные характеристики надежности невосстанавливаемых и восстанавливаемых изделий;

- изучить законы распределения, используемые в исследованиях и расчетах надежности; методы статистической оценки надежности изделий в условиях эксплуатации; методику построения структурных моделей надежности и ее расчета; методику разработки требований к надежности ИС и БД.

10. Место учебной дисциплины в структуре ОПОП:

Дисциплина «Анализ защищенности информационных систем» относится к блоку Б1 части, формируемой участниками образовательных отношений по специальности 10.05.04 – Информационно-аналитические системы безопасности.

Дисциплина «Анализ защищенности информационных систем» базируется на знаниях, полученных в рамках изучения дисциплин «Тактики и техники реализации компьютерных атак», «Системы обнаружения и предотвращения компьютерных атак (IDS/IPS)», «Безопасность автоматизированных систем управления технологическим процессом», а также дисциплин, изучающих информационную безопасность. Приобретенные в результате обучения знания, умения и навыки используются при изучении дисциплин «Технологии разведки по открытым источникам данных (OSINT)», «Расследование инцидентов информационной безопасности и правонарушений в компьютерной сфере», а также в различных практиках и при написании выпускной квалификационной работы.

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

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ПК-2	Способен организовывать работы по выполнению в информационно-аналитических системах требований защиты информации ограниченного доступа	ПК-2.1	Способен анализировать безопасность информации с помощью формальных моделей.	Знать: способы и методы анализа безопасности информации с помощью формальных моделей; Уметь: моделировать угрозы безопасности информации; Владеть: навыками анализа защищенности информационных систем.
		ПК-2.3	Способен анализировать защищенность информационных систем	

12. Объем дисциплины в зачетных единицах/часах
— 5/180.
Форма промежуточной аттестации экзамен.

13. Трудоемкость по видам учебной работы:

Вид учебной работы	Трудоемкость (часы)	
	Всего	По семестрам
		8 сем.
Контактная работа	96	96
в том числе: лекции	48	48
практические	–	–
лабораторные	48	48
курсовая работа		
Самостоятельная работа	48	48
Промежуточная аттестация-экзамен	36	36
Итого:	180	180

13.1. Содержание дисциплины:

№ п/п	Наименование раздела дисциплины		Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции				
1.1	Политика безопасности информационных систем	Перечень нормативно-методических и организационно-распорядительных документов по защите информации на предприятии.	Перечень нормативно-методических документов по защите информации на предприятии. Перечень организационно-распорядительных документов по защите информации на предприятии.	-
1.2		Назначение и содержание политики информационной безопасности предприятия в целом, его структурных подразделений, и частных политик безопасности.	Назначение и содержание политики ИБ предприятия в целом. Назначение и содержание политики информационной безопасности структурных подразделений предприятия, частных политик безопасности.	-
1.3		Средства реализации частных политик безопасности.	Разработка политики безопасности организации. Средства реализации частных политик безопасности.	-
1.4		Типичные угрозы информации и уяз-	Угрозы безопасности информации от несанкционированного доступа.	

		вимости корпоративных автоматизированных систем.	Угрозы безопасности информации по техническим каналам.	
1.5		Модель нарушителя политики безопасности.	Основные аспекты модели нарушителя политики безопасности. Порядок оформления модели нарушителя политики безопасности.	
1.6		Разграничение полномочий и ответственности персонала, обеспечивающего реализацию положений нормативно-методических и организационно-распорядительных документов по защите информации на предприятии.	Разграничение полномочий и ответственности персонала. Уголовная и административная ответственность.	
1.7	Методы и средства обеспечения информационной безопасности компьютерных систем	Компьютерная система как объект информационной безопасности. Общая характеристика методов и средств защиты информации.	Основные принципы обеспечения информационной безопасности в АС. Основные методы и средства защиты информации	-
1.8		Организационно-правовые, технические и криптографические методы обеспечения информационной безопасности.	Информация как объект правового регулирования. Организационно-правовые методы обеспечения информационной безопасности. Криптографические методы обеспечения информационной безопасности. Технические методы обеспечения информационной безопасности. Программно-аппаратные средства обеспечения информационной безопасности: СЗИ Secret Net; СЗД Панцирь; СЗИ Страж NT.	-
2. Лабораторные занятия				
2.1	Политика безопасности информационных	Сущность и понятие защиты информации	Анализ источников, каналов распространения и каналов утечки информации; Проведение анализа информации на предмет целостности; Оценка уязвимости информации.	-
2.2		Основы защиты информации	Требования к безопасности информационных систем;	-

	систем		Требования к безопасности информационных систем в России; Оценка состояния безопасности ИС США; Определение классов защищенности средств вычислительной техники от несанкционированного доступа; Определение требований к защите информации.	
2.3		Правовое обеспечение информационной безопасности	Анализ терминов и определений информационной безопасности; Работа с ГОСТами в области информационной безопасности.	-
2.4	Методы и средства обеспечения информационной безопасности компьютерных систем	Организационные основы защиты информации	Составление инструкции по обработке и хранению конфиденциальных документов; Определение коэффициента важности, полноты, адекватности, релевантности, толерантности информации; Оценка безопасности информации на объектах ее обработки.	-
2.5		Обеспечение безопасности автоматизированных систем	Классификация автоматизированных систем обработки информации по классу защиты информации; Планирование, создание и изменение учетных записей пользователей; Создание и администрирование групп пользователей; Планирование и установка разрешений NTFS для файлов, папок отдельным пользователям и группам; Наследование разрешений в NTFS; Изменение параметров учетных записей пользователей; Настройка политики учетных записей; Настройка параметров безопасности операционных систем; Настройка параметров безопасности Windows; Настройка параметров безопасности Интернет.	-

13.2. Темы (разделы) дисциплины и виды занятий:

№ п/п	Наименование раздела дисциплины	Виды занятий (количество часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
01	Политика безопасности информационных систем.	36	-	20	32	88
02	Методы и средства обеспечения информационной безопасности компьютерных систем	12	-	28	16	56
Итого		48	-	48	48	144

14. Методические указания для обучающихся по освоению дисциплины:

В процессе преподавания дисциплины используются такие виды учебной работы, как лекции и лабораторные занятия, а также различные виды самостоятельной работы обучающихся.

Методические указания к лекционным занятиям

В ходе лекционных занятий студентам необходимо внимательно слушать и вести конспектирование учебного материала. Обращать внимание на определения, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции при самостоятельном разборе материала, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

После каждой лекции студентам рекомендуется подробно разобрать прочитанный теоретический материал, выучить все определения и формулировки, разобрать примеры, решенные на лекции. Перед следующей лекцией обязательно повторить материал предыдущей лекции.

Преподаватель может (выборочно) проверить конспекты лекций.

Методические рекомендации студентам к лабораторным занятиям

Важной составной частью учебного процесса в вузе являются лабораторные занятия. Лабораторные занятия требуют помимо знаний теоретического материала еще и навыков решения практических задач, и помогают студентам глубже усвоить учебный материал, приобрести и закрепить практические навыки и навыки творческой работы над учебной и научной литературой.

Перед лабораторным занятием обязательно повторить лекционный материал, основные понятия по темам, изучить примеры.

В начале лабораторного занятия происходит обсуждение темы текущего лабораторного занятия, рассмотрение примеров и задач, рекомендации по выполнению лабораторной работы. Это возможность для студентов обратить внимание на непонятные моменты и разобрать их. Также преподавателем сообщается рекомендуемая литература, цель и задачи ее изучения.

Далее преподавателем выдаются индивидуальные задания для выполнения лабораторной работы, и студенты приступают к выполнению заданий, используя изученные теоретические положения. По окончании выполнения лабораторной работы студент оформляет отчет, содержащий тему работы, цель, задание,

описание решения, результаты, соответствующие выводы по полученным результатам, список использованной литературы.

После оформления отчета студенту необходимо защитить результаты выполнения лабораторной работы по контрольным вопросам, соответствующим теме работы. В процессе защиты студенты под руководством преподавателя более глубоко осмысливают теоретические положения, методы выполнения, полученные результаты по теме занятия. На защите результатов лабораторной работы студент должен быть готовым к ответам на все теоретические вопросы рассматриваемой темы, проявлять максимальную активность, осознанно и логически обоснованно формулировать выводы. Ответы должны строиться свободно, убедительно и аргументировано. Преподаватель следит, чтобы ответы были точными, логично построенными и не сводились к чтению конспекта. Необходимо, чтобы студент проявлял глубокое понимание того, о чем он говорит, сопоставлял теоретические знания с их практическим применением для решения задач, был способен привести конкретные примеры тех положений, о которых рассуждает теоретически. Преподавателю необходимо внимательно и критически слушать, подмечать недостатки и ошибки, корректировать их. При этом обратить внимание на то, что еще не было сказано, или поддержать и направить на развитие оригинальной мысли, высказанной студентом.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины:

а) основная литература:

№ п/п	Источник
1	Голуб, Владимир Александрович. Информационная безопасность компьютерных систем. Защита целостности информации : учебное пособие для вузов / В.А. Голуб ; Воронеж. гос. ун-т. Воронеж : ЛОП ВГУ, 2006. 31 с. (23 экз.)
2	Минзов, А. С. Информационная безопасность и защита информации [Электронный ресурс] : практикум / Минзов А. С., Бобылева С. В., Осипов П. А., Попов А. А. Дубна : Гос. ун-т «Дубна», 2020 85 с. https://e.lanbook.com/book/154490 ISBN 978-5-89847-608-3
3	Ковалев, Д. В. Информационная безопасность : учебное пособие / Д. В. Ковалев, Е. А. Богданова ; Южный федеральный университет Ростов-на-Дону : ЮФУ, 2016 74 с. : Режим доступа: электронная библиотечная система «Университетская библиотека ONLINE», требуется авторизация https://biblioclub.ru/index.php?page=book&id=493175 ISBN 978-5-9275-2364-1

б) дополнительная литература:

№ п/п	Источник
1.	Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова ; Самарский гос. архитектурно-строит. ун-т Самара : СГАСУ, 2014 113 с. : Режим доступа: электронная библиотечная система «Университетская библиотека ONLINE», требуется авторизацияhttps://biblioclub.ru/index.php?page=book&id=438331 ISBN 978-5-9585-0603-3
2.	Пакин, А. И. Информационная безопасность информационных систем управления предприятием : учебное пособие / А. И. Пакин Москва : Альтаир|МГАВТ, 2009 41 с. Режим доступа: электронная библиотечная система «Университетская библиотека ONLINE», требуется автори-

	зация https://biblioclub.ru/index.php?page=book&id=429778
3.	Артемов, А. В. Информационная безопасность: курс лекций : курс лекций / А. В. Артемов ; МАБВ Орел : 2014 257 с. Режим доступа: электронная библиотечная система «Университетская библиотека ONLINE», требуется авторизация https://biblioclub.ru/index.php?page=book&id=428605
4.	Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова ; Самарский гос. архитектурно-строит. ун-т Самара : 2014 113 с. Режим доступа: электронная библиотечная система «Университетская библиотека ONLINE», требуется авторизация https://biblioclub.ru/index.php?page=book&id=438331 ISBN 978-5-9585-0603-3
5.	*Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов ; НГТУ. Новосибирск : 2019. 83 с. ISBN 978-5-7782-3918-0.*
6.	*Башлы, П. Н.Информационная безопасность: учебно-практическое пособие : учебное пособие / П. Н. Башлы, Е. К. Баранова, А. В. Бабаш Москва : Евразийский открытый институт, 2011 375 с. Режим доступа: электронная библиотечная система «Университетская библиотека ONLINE», требуется авторизация https://biblioclub.ru/index.php?page=book&id=90539ISBN 978-5-374-00301-7*
7.	*Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие / В. Я. Ищейнов Москва, Берлин : Директ-Медиа, 2020 271 с. : схем., табл. Библиогр. в кн. Режим доступа: электронная библиотечная система «Университетская библиотека ONLINE», требуется авторизация https://biblioclub.ru/index.php?page=book&id=571485https://doi.org/10.23681/571485ISBN 978-5-4499-0496-610.23681/571485*
8.	*Спицын, В. Г.Информационная безопасность вычислительной техники : учебное пособие / В. Г. Спицын ; Томский Государственный университет систем управления и радиоэлектроники (ТУСУР)Томск : Эль Контент, 2011 148 с. : ил.,табл., схем. Режим доступа: электронная библиотечная система «Университетская библиотека ONLINE», требуется авторизация https://biblioclub.ru/index.php?page=book&id=208694ISBN 978-5-4332-0020-3*
9.	*Информационная безопасность в цифровом обществе: учебное пособие / А. С. Исмагилова, И. В. Салов, И. А. Шагапов, А. А. Корнилова Уфа : Башкирский гос. ун-т, 2019 128 с. Режим доступа: электронная библиотечная система «Университетская библиотека ONLINE», требуется авторизация https://biblioclub.ru/index.php?page=book&id=611084*
10.	*Информационная безопасность = Information Security : журнал. Москва : Гротек.*

в) информационные электронно-образовательные ресурсы**:**

№ п/п	Источник
11.	*Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/)*
12.	*http://www.math.vsu.ru – официальный сайт математического факультета ВГУ*
13.	*Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. —* <URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-

	dokumenty/bazovaya-model-ot-15-fevralya-2008-g >.
14.	*Электронный фонд актуальных правовых и нормативно-технических документов. https://docs.cntd.ru/*
15.	*Стандарт США «Критерии оценки гарантированно защищенных вычислительных систем в интересах министерства обороны США» https://prog.bobrodobro.ru/hcITwkOadFEw*
16.	*ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Методы и средства обеспечения безопасности» .—* <URL: https://docs.cntd.ru/document/1200051499/titles >.
17.	*Google, Yandex, Rambler*

16. Перечень учебно-методического обеспечения для самостоятельной работы:

Курс дисциплины построен таким образом, чтобы позволить студентам максимально проявить способность к самостоятельной работе. Для успешной самостоятельной работы предполагается тесный контакт с преподавателем.

Изучение дисциплины следует начинать с проработки настоящей рабочей программы, особое внимание, уделяя целям и задачам, структуре и содержанию курса.

Студентам рекомендуется получить в библиотеке учебную литературу по дисциплине, необходимую для эффективной работы на всех видах аудиторных занятий, а также для самостоятельной работы по изучению дисциплины.

Своевременное и качественное выполнение самостоятельной работы базируется на соблюдении настоящих рекомендаций и изучении рекомендованной литературы. Студент может дополнить список использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы при написании курсовых и дипломных работ.

Успешное освоение курса предполагает активное, творческое участие студента путем планомерной, повседневной работы.

№ п/п	Источник
1	Коллеров, А. С. Информационная безопасность [Электронный ресурс] : учебное пособие / Коллеров А. С. Екатеринбург : ЕАСИ, 2014 183 с. Книга из коллекции ЕАСИ - Информатикаhttps://e.lanbook.com/book/136383 ISBN 978-5-904440-33-6
2	Бурова, М. А. Информационная безопасность и криптографическая защита информации [Электронный ресурс] : конспект лекций / Бурова М. А. Самара : СамГУПС, 2009 98 с. Книга из коллекции СамГУПС - Информатикаhttps://e.lanbook.com/book/130271 Информационная безопасность и защита информации / Бурова М. А., Овсянников А. С. Ч. 1,2: Информационная безопасность и защита информации. Ч. 2 : конспект лекций. Ч. 2 / Бурова М. А., Овсянников А. С. Самара : СамГУПС, 2012 150 с. Книга из коллекции СамГУПС - Информатикаhttps://e.lanbook.com/book/130272
3	Лойко, В. И. Информационная безопасность [Электронный ре-

	сурс] : учебное пособие / Лойко В. И.,Лаптев В. Н.,Аршинов Г. А.,Лаптев С. Н. Краснодар : КубГАУ, 2020 332 с. Книга из коллекции КубГАУ - Информатикаhttps://e.lanbook.com/book/254168 ISBN 978-5-907346-50-5
4	Полутова, М. А. Информационная безопасность и защита персональных данных сотрудников [Электронный ресурс] : монография / Полутова М. А.,Стельмашенко О. В.,Александрова Н. А.,Антонова В. С. Чита : ЗабГУ, 2022 250 с. Книга из коллекции ЗабГУ - Информатикаhttps://e.lanbook.com/book/363386 ISBN 978-5-9293-3178-7
5	Положение об организации самостоятельной работы обучающихся в Воронежском государственном университете

17. Образовательные технологии, используемые для реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ, электронное обучение (ЭО), смешанное обучение)

Изложение учебного материала основано на принципе системности, преемственности и последовательности и направлено на развитие интеллектуальных умений, профессиональных компетенций студентов.

Лекционные и лабораторные занятия ведутся с привлечением мультимедийных технологий. Практические работы выполняются на компьютерной технике с использованием различных информационных технологий. Осуществляется интерактивная связь с преподавателем через сеть интернет, проводятся индивидуальные онлайн консультации.

Перечень необходимого программного обеспечения: операционная система Windows, Microsoft LibreOffice, браузер Mozilla Firefox, Opera или Internet Expolorer, экран, ноутбук, мультимедиапроектор.

18. Материально-техническое обеспечение дисциплины:

Учебная аудитория для проведения занятий лекционного и семинарского типа, текущего контроля и промежуточной аттестации; специализированная мебель. Компьютерный класс: специализированная мебель, маркерная доска, персональные компьютеры

Ubuntu (бесплатное и/или свободное ПО, лицензия: https://ubuntu.com/download/desktop)

Visual Studio Community (бесплатное и/или свободное ПО, лицензия https://visualstudio.microsoft.com/ru/vs/community/)

LibreOffice (GNU Lesser General Public License (LGPL), бесплатное и/или свободное ПО, лицензия: https://ru.libreoffice.org/about-us/license/)

Для самостоятельной работы используются классы с компьютерной техникой, оснащенные необходимым программным обеспечением, электронными учебными пособиями и законодательно-правовой и нормативной поисковой системой, имеющий выход в глобальную сеть.

19. Оценочные средства для проведения текущей и промежуточной аттестаций:

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	Политика безопас-	ПК-2	ПК-2.1	Опрос по лабораторным ра-

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
	ности информационных систем		ПК-2.3	ботам и материалам лекций
2.	Методы и средства обеспечения информационной безопасности компьютерных систем	ПК-2	ПК-2.1 ПК-2.3	Опрос по лабораторным работам и материалам лекций
Промежуточная аттестация форма контроля – экзамен				КИМы к экзамену

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на занятиях.

Задание для текущего контроля и проведения промежуточной аттестации должны быть направлены *на оценивание:*

1. уровня освоения теоретических и практических понятий, научных основ профессиональной деятельности;

2. степени готовности обучающегося применять теоретические и практические знания и профессионально значимую информацию, сформированности когнитивных умений.

3. приобретенных умений, профессионально значимых для профессиональной деятельности.

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

Примерный перечень заданий

Раздел 1

1. Анализ источников, каналов распространения и каналов утечки информации;

2. Проведение анализа информации на предмет целостности;

3. Оценка уязвимости информации;

4. Определение классов защищенности средств вычислительной техники от несанкционированного доступа;

5. Определение требований к защите информации;

Раздел 2

1. Составление инструкции по обработке и хранению конфиденциальных документов.

2. Определение коэффициента важности, полноты, адекватности, релевантности, толерантности информации.

3. Оценка безопасности информации на объектах ее обработки.

4. Классификация автоматизированных систем обработки информации по классу защиты информации.

5. Создание и администрирование групп пользователей.

6. Изменение параметров учетных записей пользователей.
7. Настройка политики учетных записей.
8. Настройка параметров безопасности операционных систем.
9. Настройка параметров безопасности Windows.
10. Настройка параметров безопасности Интернет.

Описание технологии проведения

Текущий контроль предназначен для проверки хода и качества формирования компетенций, стимулирования учебной работы обучаемых и совершенствования методики освоения новых знаний. Он обеспечивается проведением защит отчетов по лабораторным работам и опроса по результатам их выполнения. При текущем контроле уровень освоения учебной дисциплины и степень сформированности компетенции определяются оценками «зачтено» и «незачтено».

Для оценивания текущего контроля успеваемости
используются следующие показатели:

1) знание основных понятий и методов;

2) умение применять полученные знания и навыки для решения задач, проводить анализ полученных решений.

Шкала оценок:

Зачтено: Выполнение заданий соответствует перечисленным показателям, обучающийся дает ответы на дополнительные вопросы, может быть не совсем полные. Демонстрирует умение решать задачи, возможно с некоторыми ошибками.

Не зачтено: Ответы не соответствуют ни одному из перечисленных показателей. Обучающийся демонстрирует фрагментарные знания и умения или их отсутствие

Если текущая аттестация проводится в дистанционном формате, то у обучающийся обязательно должен иметь компьютер, микрофон, камеру, необходимые программные средства и информационные технологии для реализации решения практических заданий. Если у обучающегося отсутствует необходимое оборудование, то он обязан сообщить преподавателю об этом за 3 суток.

20.2 Промежуточная аттестация

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

Промежуточная аттестация предназначена для определения уровня освоения всего объема учебной дисциплины. Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

Перечень теоретических вопросов к экзамену

Номер вопроса	Текст вопроса
1	Перечень нормативно-методических документов по защите информации на предприятии.
2	Перечень организационно-распорядительных документов по защите информации на предприятии.
3	Назначение и содержание политики ИБ предприятия в целом

4	Назначение и содержание политики информационной безопасности структурных подразделений предприятия, частных политик безопасности
5	Разработка политики безопасности организации.
6	Средства реализации частных политик безопасности.
7	Угрозы безопасности информации от несанкционированного доступа.
8	Угрозы безопасности информации по техническим каналам.
9	Основные аспекты модели нарушителя политики безопасности.
10	Порядок оформления модели нарушителя политики безопасности.
11	Разграничение полномочий персонала.
12	Уголовная и административная ответственность.
13	Компьютерная система как объект информационной безопасности.
14	Основные принципы обеспечения информационной безопасности в АС.
15	Основные методы и средства защиты информации.
16	Информация как объект правового регулирования
17	Организационно-правовые методы обеспечения информационной безопасности
18	Криптографические методы обеспечения информационной безопасности.
19	Технические методы обеспечения информационной безопасности.
20	Программно-аппаратные средства обеспечения информационной безопасности.
21	СЗИ Secret Net.
22	СЗД Панцирь.
23	СЗИ Страж NT.

Перечень практических заданий

Тема 1

6. Анализ источников, каналов распространения и каналов утечки информации;

7. Проведение анализа информации на предмет целостности;

8. Оценка уязвимости информации;

9. Определение классов защищенности средств вычислительной техники от несанкционированного доступа;

10. Определение требований к защите информации;

Тема 2

1. Составление инструкции по обработке и хранению конфиденциальных документов.

2. Определение коэффициента важности, полноты, адекватности, релевантности, толерантности информации.

3. Оценка безопасности информации на объектах ее обработки.

4. Классификация автоматизированных систем обработки информации по классу защиты информации.

5. Создание и администрирование групп пользователей.

6. Изменение параметров учетных записей пользователей.

7. Настройка политики учетных записей.

8. Настройка параметров безопасности операционных систем.

9. Настройка параметров безопасности Windows.

10. Настройка параметров безопасности Интернет.

Примерное содержание Контрольно-измерительных материалов

УТВЕРЖДАЮ
заведующий кафедрой теории функций и геометрии
_Семенов Е.М.__
подпись, расшифровка подписи
15.06.20__

Направление подготовки / специальность _10.05.04_
шифр, наименование
Дисциплина____Анализ защищенности информационных систем_____
Вид контроля _____Экзамен_____
промежуточный контроль - аттестация, зачет; текущий контроль с указанием формы
Вид аттестации _промежуточный_____
текущая, промежуточная

Контрольно-измерительный материал №_1_

Теория:

1. Перечень нормативно-методических документов по защите информации на предприятии.
2. Угрозы безопасности информации по техническим каналам.
3. СЗД Панцирь.

Практика:

1. Для объекта «Бухгалтерия» спланировать, создать и, предусмотреть изменение учетных записей пользователей.

Доцент Шипилова Е.А.
подпись расшифровка подписи

ТВЕРЖДАЮ
заведующий кафедрой теории функций и геометрии
_Семенов Е.М.__
подпись, расшифровка подписи
15.06.20__

Направление подготовки / специальность _10.05.04_
шифр, наименование
Дисциплина____Анализ защищенности информационных систем_____
Вид контроля _____Экзамен_____
промежуточный контроль - аттестация, зачет; текущий контроль с указанием формы
Вид аттестации _промежуточный_____
текущая, промежуточная

Контрольно-измерительный материал №_2_

Теория:

1. Назначение и содержание политики ИБ предприятия в целом.
2. Информация как объект правового регулирования.
3. СЗИ Страж NT.

Практика:

1. Оценить безопасность информации на объекте «Отдел кадров».

Доцент Шипилова Е.А.
подпись *расшифровка подписи*

Описание технологии проведения

Промежуточная аттестация по дисциплине «Анализ защищенности информационных систем» проводится в форме экзамена.

Промежуточная аттестация, как правило, осуществляется в конце семестра. Результаты текущей аттестации обучающегося по решению кафедры могут быть учтены при проведении промежуточной аттестации. При несогласии студента, ему дается возможность пройти промежуточную аттестацию (без учета его текущих аттестаций) на общих основаниях.

К промежуточной аттестации допускаются студенты, выполнившие и защитившие все, предусмотренные планом лабораторные работы, и прошедшие все этапы текущей аттестации с оценкой «зачтено». В случае отсутствия не более двух контрольных параметров, студент может быть допущен к промежуточной аттестации с добавлением двух дополнительных вопросов к типовому КИМ промежуточной аттестации.

Промежуточная аттестация проводится в формате собеседования с преподавателем. Обучающийся получает 3 теоретических вопроса и практическую задачу по изучаемому предмету. Время подготовки к ответу не должно превышать 1 час. При желании, студент может начать ответ без подготовки. При необходимости, преподаватель может задавать уточняющие, а в случае отсутствия оценки по контрольным точкам дополнительные вопросы.

На основании критериев оценивания, приведенных ниже, преподаватель выставляет обучающемуся оценку по дисциплине.

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

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок

- даны исчерпывающие и обоснованные ответы на вопросы, поставленные КИМ; - правильно решена задача и показано умение грамотно применять полученные теоретические знания в практических целях; - показаны твердые навыки в принятии решений или действий в созданной на экзамене обстановке; - показано глубокое и творческое овладение основной и дополнительной литературой; - высказываемые положения, решения и действия обоснованы с уверенным использованием компьютерной техники; - ответы отличаются четкостью и краткостью, действия быстротой, правильностью и решительностью, мысли и решения излагаются с применением специальной терминологии, в необходимой логической последовательности.	Повышенный уровень	**«отлично»**
- даны полные, достаточно глубокие и обоснованные ответы не вопросы, поставленные в КИМ; - правильно решена задача, но ход ее решения не является оптимальным; - показаны достаточно уверенные навыки принятия решений или действий в созданной на экзамене обстановке; - показаны достаточно прочные практические навыки; - даны полные, но недостаточно обоснованные ответы на дополнительные вопросы; - показаны глубокие знания основной и недостаточные знания дополнительной литературы; - показано умение обосновывать высказываемые положения с достаточно уверенным использованием компьютерной техники; - ответы в основном были крат-	Базовый уровень	**«хорошо»**

кими, но в них не всегда выдерживалась логическая последовательность.		
- даны в основном правильные ответы на все вопросы КИМ, но без должной глубины и обоснования; - в решении задачи допущены отдельные ошибки, не приведшие к большим отклонениям от правильного ответа; - показаны недостаточно уверенные навыки принятия решений или действий в созданной на экзамене обстановке; - показаны недостаточно прочные практические навыки; - не даны положительные ответы на дополнительные вопросы; - показаны недостаточные знания основной литературы; - при ответах неуверенно использовалась компьютерная техника; - ответы были многословными или очень краткими, мысли излагались недостаточно четко и без должной логической последовательности.	Пороговый уровень	**«удовлетворительно»**
фрагментарные знания или отсутствие знаний и умений.	-	**«неудовлетворительно»**

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

Задания закрытого типа - средний уровень сложности (один правильный ответ)

1. Персональные данные - это
   a документ, удостоверяющий соответствие объекта требованиям технических регламентов, положениям стандартов или условиям договоров
   b любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу
   c обозначение, служащее для информирования приобретателей о соответствии объекта сертификации требованиям системы добровольной сертификации или национальному стандарту
2. Какой орган исполнительной власти является уполномоченным в области противодействия технической разведке и технической защиты информации
   a Федеральная служба по техническому и экспортному контролю Российской Федерации (ФСТЭК России)

b Федеральная служба безопасности
c органы законодательной, исполнительной и судебной власти

3. Нарушитель - это
   a субъект, имеющий доступ к помещению, аттестованному как «секретное»
   b субъект, имеющий доступ на объект обработки персональной информации
   c субъект, имеющий доступ к работе со штатными средствами АС или СВТ как части АС
4. Межсетевой экран (МЭ) представляет собой
   a локальное (однокомпонентное) или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации
   b общесистемное программное средство
   c соединенные каналами связи системы обработки данных, ориентированные на конкретного пользователя
5. Информация для служебного пользования – это
   a информация, которая используется персоналом для функционирования организации
   b информация, которая может свободно распространяться для общественного использования через авторизованные каналы организации
   c информация с грифом «секретно»

Компетенция	Вопрос	Ответ	√
ПК-2.1. Способен анализировать безопасность информации с помощью формальных моделей *Задания закрытого типа - средний уровень сложности*	1. Свободно доступная информация – это	информация, которая используется персоналом для функционирования организации	
		информация с грифом «секретно»	
		информация, которая может свободно распространяться для общественного использования через авторизованные каналы организации	√
	2. Модель защиты (безопасности) – это	**абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и (или) организационных мер защиты от несанкционированного доступа**	√
		информация, которая может свободно распространяться для общественного использования через авторизованные каналы организации	

		информация, которая используется персоналом для функционирования организации	
	3. Какие компоненты включает в себя политика безопасности организации	роли и ответственность сотрудников организации в обеспечении безопасности	
		базовая политика безопасности	√
		процедуры безопасности	√
		специализированные политики безопасности	√
ПК-2.3. Способен анализировать защищенность информационных систем *Задания закрытого типа - средний уровень сложности*	1. Оценка риска выявляет	как наиболее ценные, так и наиболее уязвимые активы	√
		гарантии безопасности, аудит и средства контроля	
		средства контроля и аудита	
	2. Полномочия системного администратора позволяют	выполнять действия, необходимые для управления безопасностью	
		выполнить все действия, необходимые для управления компьютерными системами	√
		выполнять отдельные действия по модификации конфигурации системы	

Требования к выполнению заданий, шкалы и критерии оценивания

1) Тестовые задания.

<u>- Задания закрытого типа – средний уровень сложности (выбор одного варианта ответа, верно/неверно):</u>

- 1 балл – указан верный ответ;
- 0 баллов – указан неверный ответ.

<u>- Задания закрытого типа - средний уровень сложности (множественный выбор):</u>

- 2 балла – указаны все верные ответы;
- за каждый верный ответ ставится 1 балл, при этом за каждый неверный ответ вычитается 1 балл;
- 0 баллов — не выбрано ни одного верного ответа.

<u>- Задания закрытого типа (на соответствие):</u>

- 2 балла – все соответствия определены верно;
- за каждое верное сопоставление ставится количество баллов, равное максимальному (2 балла), деленному на количество предлагаемых в вопросе сопоставлений;
- 0 баллов – ни одно сопоставление не выбрано верно.

<u>- Задания открытого типа (короткий ответ):</u>

- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ.