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

УТВЕРЖДАЮ
заведующий кафедрой
кибербезопасности
информационных систем
С.Л. Кенин

22.03.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ Б1.В.05 Правовые аспекты информационной безопасности

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

"Безопасность компьютерных систем и сетей" (по отрасли или в сфере профессиональной деятельности)

3. Квалификация (степень) выпускника: Специалист

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:

кибербезопасности информационных систем

6. Составители программы:

Кенин Сергей Леонидович, к.т.н., доцент кафедры кибербезопасности информационных систем

7. Рекомендована:
НМС факультета ПММ, протокол № 8 от 15.04.2022
Внесены изменения: протокол УС факультета ПММ, протокол № 8 от 27.02.2024
Рекомендована с изменениями: протокол НМС факультета ПМ, протокол № 5 от 22.03.2024

8. Учебный год: 2025/2026 **Семестр(ы):** 8

9. Цели и задачи учебной дисциплины

Формирование профессиональных навыков, связанных со структурой политико-правового обеспечения информационной безопасности и соответствующего законодательства в области информации, информационных технологий и защиты информации, персональных данных, государственной тайны, ЭЦП, технического регулирования; понятий, связанных с вопросами ответственности за правонарушения в области информационной безопасности, а также механизмами защиты прав и законных интересов субъектов информационной сферы.

10. Место учебной дисциплины в структуре ОПОП: дисциплина относится к вариативной части блока Б1 дисциплин учебного плана.

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)	Индикаторы(ы)	Планируемые результаты обучения
ПК-3	Способен участвовать в работах по проектированию систем защиты информации в компьютерных системах и сетях при решении профессиональных, исследовательских и прикладных задач	ПК-3.1	владеет знаниями международных и отечественных нормативно-правовых актов, стандартов и правил в области информационных технологий и информационной безопасности	Знает: международные и отечественные нормативно-правовые акты, стандарты и правила в области информационных технологий и информационной безопасности. Владеет: знаниями международных и отечественных нормативно-правовых актов, стандартов и правил в области информационных технологий и информационной безопасности

12. Объем дисциплины в зачетных единицах/час - 3/108.
Форма промежуточной аттестации - зачет.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоёмкость (часы)					
	Всего	В том числе в интерактивной форме	По семестрам			
			8			
Аудиторные занятия	42		42			
в том числе: лекции	14		14			
Практические	28		28			
Лабораторные	0		0			
Самостоятельная работа	66		66			
Контроль	0		0			
Итого:	108		108			
Форма промежуточной аттестации	Зачет		Зачет			

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Информация как объект правового регулирования	Субъекты и объекты правоотношений в области информационной безопасности. Формирование информационных ресурсов и их квалификация. Конституционные гарантии прав на информацию и механизм их реализации.	https://edu.vsu.ru/course/)
1.2	Законодательство в области информационной безопасности.	Отрасли законодательства, регламентирующие деятельность по защите информации. Доктрина информационной безопасности России. Перспективы развития законодательства в области информационной безопасности.	
1.3	Правовой режим защиты государственной тайны.	Принципы, механизм и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Органы защиты государственной тайны и их компетенция. Порядок допуска и доступа к государственной тайне. Иные меры по обеспечению сохранности сведений, составляющих государственную тайну (режим секретности как основной порядок деятельности в сфере защиты государственной тайны). Перечень и содержание организационных мер, направленных на защиту государственной тайны. Система контроля за состоянием защиты государственной тайны. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная).	
1.4	Правовые режимы защиты конфиденциальной информации.	Правовые режимы конфиденциальной информации: содержание и особенности. Основные требования, предъявляемые к организации защиты конфиденциальной информации. Юридическая ответственность за нарушения правового режима конфиденциальной информации (уголовная, административная, гражданско-правовая, дисциплинарная).	
1.5	Организационное обеспечение ИБ.	Подразделения, обеспечивающие информационную безопасность предприятия, организации. Обзор российских национальных стандартов в сфере информационной безопасности. Понятие «режим защиты информации». Политика информационной	

		безопасности.	
1.6	Защита интеллектуальной собственности.	Понятие интеллектуальной собственности. Объекты и субъекты авторского права. Исключительные авторские права. Смежные права. Правовая охрана программ для ЭВМ, баз данных и топологий интегральных микросхем. Защита авторских и смежных прав. Основы патентных правоотношений. Условия патентоспособности. Объекты изобретения, связанные с электронно-вычислительной техникой и информационными технологиями. Авторы изобретений и патентообладатели. Механизм патентования. Защита прав патентообладателей и авторов. Особенности договорных отношений в области информационной безопасности. Правовое регулирование взаимоотношений администрации и персонала в области обеспечения информационной безопасности. Особенности трудовых отношений.	
1.7	Международное законодательство в области защиты информации	Субъекты и объекты международного информационного обмена. Национальные законодательства о компьютерных правонарушениях и защите информации. (Беларусь, США, ЕС, Китай). Международное сотрудничество в области борьбы с компьютерной преступностью.	
1.8	Компьютерные правонарушения	Признаки и элементы состава преступления. Основы расследования преступлений в сфере компьютерной информации. Административная ответственность за правонарушения в сфере информационных технологий. Обзор положений ГОСТ Р ИСО/МЭК 18044-2007 «Менеджмент инцидентов информационной безопасности» для решения задач расследования инцидентов безопасности.	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)					
		Лекции	Практ.	Лаб. раб.	Самостоятельная работа	Контроль	Всего
1.1	Информация как объект правового регулирования	1	0	0	6	0	7
1.2	Законодательство в области информационной безопасности.	1	2	0	10	0	13
1.3	Правовой режим защиты государственной тайны.	2	4	0	8	0	14
1.4	Правовые режимы защиты конфиденциальной информации.	2	4	0	8	0	14
1.5	Организационное обеспечение ИБ.	2	4	0	8	0	14
1.6	Защита интеллектуальной собственности.	2	6	0	10	0	18
1.7	Международное законодательство в области защиты информации	2	2	0	6	0	10
1.8	Компьютерные правонарушения	2	6	0	10	0	18
	Итого:	14	28	0	66	0	108

14. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины включает в себя лекционные занятия, лабораторные занятия и самостоятельную работу обучающихся. На первом занятии студент получает информацию для доступа к комплексу учебно-методических материалов.

Лекционные занятия посвящены рассмотрению теоретических основ дисциплины.

Лабораторные занятия предназначены для формирования умений и навыков, закрепленных компетенциями по ОПОП. Самостоятельная работа студентов включает в себя проработку учебного материала лекций, разбор лабораторных заданий, подготовку к экзамену.

Для успешного освоения дисциплины рекомендуется подробно конспектировать лекционный материал, просматривать презентации (при наличии) по соответствующей теме, изучать основную и дополнительную литературу рекомендуемой библиографии,

При использовании дистанционных образовательных технологий и электронного обучения выполнять все указания преподавателей по работе на LMS-платформе, своевременно подключаться к online-занятиям, соблюдать рекомендации по организации самостоятельной работы.

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

а) основная литература:

№ п/п	Источник
1	Организационно-правовое обеспечение информационной безопасности : учебник / А. А. Стрельцов, В. Н. Пожарский, В. А. Минаев [и др.] ; под редакцией А. А. Александрова, М. П. Сычева. — Москва : МГТУ им. Баумана, 2018. — 291 с. — ISBN 978-5-7038-4723-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/172840. — Режим доступа: для авториз. пользователей.
2	Новиков, В. К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) : учебное пособие / В. К. Новиков. — Москва : Горячая линия-Телеком, 2017. — 176 с. — ISBN 978-5-9912-0525-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111084. — Режим доступа: для авториз. пользователей.

б) дополнительная литература:

№ п/п	Источник
3	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). ФСТЭК России, 2008. https://fstec.ru/en/dokumenty/vse-dokumenty/spetsialnye-normativnyedokumenty/bazovaya-model-ot-15-fevralya-2008-g?ysclid=lj8zaq9vbh762206938
4	Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 фев 2021г.) https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnyedokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g?ysclid=lj8z58t2v2240278685
5	Коваленко, Ю. И. Правовой режим лицензирования и сертификации в сфере информационной безопасности : учебное пособие / Ю. И. Коваленко. — Москва : Горячая линия-Телеком, 2012. — 140 с. — ISBN 978-5-9912-0261-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/5163. — Режим доступа: для авториз. пользователей.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
6	Электронно-библиотечная система «Лань» - Режим доступа: https://e.lanbook.com
7	Электронный каталог Научной библиотеки Воронежского государственного университета. - Режим доступа: http//:www.lib.vsu.ru.
8	Образовательный портал «Электронныйуниверситет ВГУ». — Режим доступа: https://edu.vsu.ru

16. Перечень учебно-методического обеспечения для самостоятельной работы

В качестве формы организации самостоятельной работы применяются методические указания для самостоятельного освоения и приобретения навыков работы со специализированным программным обеспечением. Самостоятельная работа студентов: изучение теоретического материала; подготовка к лекциям, работа с учебно-методической литературой, подготовка отчётов по практическим работам, подготовка к зачету.

Для обеспечения самостоятельной работы студентов в электронном курсе дисциплины на образовательном портале «Электронный университет ВГУ» сформирован учебно-методический комплекс, который включает в себя: программу курса, учебные пособия и справочные материалы, методические указания по выполнению заданий лабораторных работ. Студенты получают доступ к данным материалам на первом занятии по дисциплине.

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

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий. Для организации занятий рекомендован онлайн-курс «Б1.В.05 Правовые аспекты информационной безопасности (10.05.01)», размещенный на платформе Электронного университета ВГУ (LMS moodle), а также Интернет-ресурсы, приведенные в п.15в.5.

18. Материально-техническое обеспечение дисциплины

Учебная аудитория для лекций: специализированная мебель, компьютер преподавателя, мультимедийный проектор, экран.
Учебная аудитория для лабораторных занятий: специализированная мебель, персональные компьютеры, мультимедийный проектор, экран, лабораторное оборудование программно-аппаратных средств обеспечения информационной безопасности.
Аудитория для самостоятельной работы: учебная мебель, компьютер с возможностью подключения к сети «Интернет» и электронной платформе Электронного университета ВГУ.

Программное обеспечение (см.файл МТО): ОС Windows v.7, 8, 10, набор утилит (архиваторы, файл-менеджеры), LibreOffice v.5-7, Foxit PDF Reader.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

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

№ п/п	Наименования раздела дисциплины	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Информация как объект правового регулирования	ПК-3	ПК-3.1	устный опрос, тест
2	Законодательство в области информационной безопасности.			устный опрос, тест, практическое задание
3	Правовой режим защиты государственной тайны.			устный опрос, тест, практическое задание
4	Правовые режимы защиты конфиденциальной информации.			устный опрос, тест, практическое задание
5	Организационное обеспечение ИБ.			устный опрос, тест, практическое задание
6	Защита интеллектуальной собственности.			устный опрос, тест, практическое задание
7	Международное законодательство в области защиты информации			устный опрос, тест, практическое задание
8	Компьютерные правонарушения			устный опрос, тест, практическое задание
Промежуточная аттестация, форма контроля - зачет				Перечень вопросов (КИМ№1)

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

- устный опрос,
- тест,
- практическое задание.

Перечень вопросов устного опроса

1. Принципы государственной политики обеспечения информационной безопасности.
2. Ключевые проблемы информационной безопасности государства.
3. Основные обязанности органов законодательной власти в сфере информационной безопасности.
4. Основные обязанности органов исполнительной власти в сфере информационной безопасности.
5. Основные обязанности органов судебной власти в сфере информационной безопасности.
6. Информационные войны: проблемы правового регулирования.
7. Право на доступ к информации в России: проблемы теории и законодательства.
8. Проблема практического применения ФЗ «Об информации, информационных технологиях и о защите информации».
9. Понятие и роль информации в жизни современного общества.
10. Гарантии информационных прав граждан.
11. Права граждан в информационной сфере.
12. Организация защиты государственной тайны в России.
13. Ответственность за шпионаж и разглашение государственной тайны.
14. Состояние и эффективность законодательства о коммерческой тайне.
15. Изменения в правовом регулировании института коммерческой тайны в связи с введением в действие четвертой части Гражданского кодекса РФ.
16. Требования к обработке персональных данных и ответственность за нарушение работы с ними.
17. Международное и национальное законодательство зарубежных стран о защите персональных данных.
18. Персональные данные в системе документооборота предприятия.
19. Персональные данные в Интернете.
20. Правовое регулирование борьбы с киберпреступностью в США (Италии, Китае, Японии, Великобритании).
21. Выявление технических каналов утечки информации.
22. История развития криптографии.
23. Криптография как средство защиты информации.
24. Расследование компьютерных преступлений в РФ и за рубежом.
25. Роль положений ГОСТ Р ИСО/МЭК 18044-2007г., «Информационная технология.
Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности», в расследовании инцидентов компьютерной безопасности.
26. Роль положений ГОСТ Р ИСО/МЭК 56824-2015 «Интеллектуальная собственность.
Использование охраняемых результатов интеллектуальной деятельности в сети Интернет» в защите интеллектуальной собственности российских государственных и коммерческих структур при ее попадании в Интернет.

Перечень практических заданий

1. Какие в настоящее время отмечаются особенности структуры информационной сферы и характеристики ее элементов?
2. В чем заключаются парадоксы понятия и структура информационной безопасности?
3. На каких принципах строятся правоотношения в области информационной безопасности?
4. В чем заключаются конституционные гарантии прав на доступ к информации и обеспечение сохранности различных видов тайны?

5. Чем обеспечиваются гарантии защиты информации по законодательству Российской федерации и исключения из предусмотренных законом правил?
6. В чем суть и основные направления реализации национальных интересов России в сфере ИБ, отраженные в Доктрине информационной безопасности Российской Федерации?
7. Каковы перспективы развития законодательства в области информационной безопасности в настоящий исторический период?
8. Каковы составляющие российской системы обеспечения безопасности критических информационных систем от компьютерных атак?
9. Каковы функции участников реализации системы обеспечения безопасности критических информационных систем от компьютерных атак?
10. На что направлено введение правового режима защиты государственной тайны?
11. Назовите состав принципов, механизмов и процедур отнесения сведений к государственной тайне, их засекречивания и рассекречивания.
12. Какие организации и структуры непосредственно осуществляют защиту государственной тайны, регулируют и контролируют?
13. Назовите и опишите порядок допуска и доступа к государственной тайне.
14. Опишите предназначение и составляющие режима секретности, как основного порядка деятельности в сфере защиты государственной тайны, организационных и технических мер, направленных на защиту государственной тайны.
15. Какими органами и в каком порядке реализуется система контроля за состоянием защиты государственной тайны?
16. Опишите составляющие условий наступления юридической ответственности за нарушения правового режима защиты государственной тайны (уголовной, административной, дисциплинарной).
17. Что общего и в чем различия в характере конфиденциальной информации различных видов: персональных данных, служебной тайны, коммерческой и банковской тайны, тайны следствия и судопроизводства, других профессиональных видов тайны?
18. Каковы основные требования, предъявляемые к организации защиты конфиденциальной информации?
19. Опишите составляющие условий наступления юридической ответственности за нарушения правового режима конфиденциальной информации (уголовной, административной, гражданско-правовой и дисциплинарной).
20. В чем отличия организационной от технической защиты информации?
21. Как определяются основные каналы утечки информации при обработке на компьютерах?
22. Как формируется и на что направлена политика информационной безопасности?
23. Опишите и дайте характеристику методов обеспечения физической безопасности._
24. Для чего вводятся и из чего состоят технологические меры поддержания безопасности?
25. Поясните на примере состав и функции подразделения, обеспечивающего информационную безопасность предприятия.
26. В чем особенности настоящего состава законодательства России об интеллектуальная собственности?
27. Поясните различие и связь исключительных авторских и смежных прав в сфере интеллектуальной собственности.
28. Какая предусмотрена в Российской Федерации правовая охрана программ для ЭВМ, баз данных и топологий интегральных микросхем?
29. Поясните сложности в защите авторских и смежных прав.
30. Какие в настоящее время условия патентоспособности действуют в настоящее время в России? В мировом сообществе?
31. Какие выделяются объекты изобретения, полезной модели и промышленного образца, связанные с электронно-вычислительной техникой и информационными технологиями?
32. Как осуществляется защита прав патентообладателей и авторов полезных моделей?
33. Каковы особенности договорных отношений России со странами ближнего и дальнего зарубежья в области информационной безопасности?
34. В чем суть и содержание правового регулирования трудовых отношений администрации и персонала в области обеспечения информационной безопасности?

35. Назовите и охарактеризуй те основные составляющие правового режима участия российских предприятий организаций и учреждений различных форм собственности в международном информационном обмене.
36. Назовите субъекты и объекты международного информационного обмена.
37. Приведите примеры положительных результатов международного сотрудничества в области борьбы с компьютерной преступностью.
38. Назовите и поясните признаки и элементы состава преступлений в сфере компьютерной информации (ст. 272, 273, 274 УК России).
39. Какие необходимо знать основы расследования преступлений в сфере компьютерной информации?
40. Каковы условия наступления административной ответственности за правонарушения в сфере информационных технологий?
41. Какие положения ГОСТ Р ИСО/МЭК 18044-2007г., «Информационная технология.
Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности» применимы в расследовании инцидентов компьютерной безопасности?
42. Какие положения ГОСТ Р ИСО/МЭК 56824-2015 «Интеллектуальная собственность. Использование охраняемых результатов интеллектуальной деятельности в сети Интернет» применимы в защите интеллектуальной собственности российских государственных и коммерческих структур при ее попадании в Интернет?

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: вопросы к зачету.

Перечень вопросов к зачету (КИМ №1)

1. Информация как объект правового регулирования. Структура информационной сферы и характеристика ее элементов. Виды информации. Формирование информационных ресурсов и их квалификация. Конституционные гарантии прав на информацию и механизм их реализации.
2. Понятие и структура информационной безопасности. Субъекты и объекты правоотношений в области информационной безопасности. Понятие и виды защищаемой информации по законодательству РФ.
3. Отрасли законодательства, регламентирующие деятельность по защите информации. Перспективы развития законодательства в области информационной безопасности.
4. Понятие правового режима защиты государственной тайны. Государственная тайна как особый вид защищаемой информации и её характерные признаки.
5. Реквизиты носителей сведений, составляющих государственную тайну. Принципы, механизм и процедура отнесения сведений к государственной тайне, их засекречивания и рассекречивания.
6. Органы защиты государственной тайны и их компетенция. Порядок допуска и доступа к государственной тайне. Иные меры по обеспечению сохранности сведений, составляющих государственную тайну (режим секретности как основной порядок деятельности в сфере защиты государственной тайны).
7. Перечень и содержание организационных мер, направленных на защиту государственной тайны. Система контроля за состоянием защиты государственной тайны. Юридическая ответственность за нарушения правового режима защиты государственной тайны (уголовная, административная, дисциплинарная).
8. Правовые режимы защиты конфиденциальной информации. Конфиденциальная информация: персональные данные, служебная тайна, коммерческая тайна, банковская тайна, тайна следствия и судопроизводства, профессиональная тайна.
9. Правовые режимы конфиденциальной информации в России: содержание и особенности. Основные требования, предъявляемые к организации защиты конфиденциальной информации. Юридическая ответственность за нарушения правового режима конфиденциальной информации (уголовная, административная, гражданско-правовая, дисциплинарная).
10. Правовая регламентация охранной деятельности. Лицензирование и сертификация в информационной сфере. Понятия лицензирования по российскому законодательству. Виды деятельности в информационной сфере, подлежащие лицензированию.

11. Правовые основы защиты информации с использованием технических средств (защиты от технических разведок, применения и разработки шифровальных средств, применения электронно-цифровой подписи и т.д.).
12. Защита интеллектуальной собственности. Законодательство РФ об интеллектуальная собственности. Понятие интеллектуальной собственности.
13. Объекты и субъекты авторского права. Исключительные авторские права. Смежные права.
14. Правовая охрана программ для ЭВМ, баз данных и топологий интегральных микросхем.
15. Защита авторских и смежных прав. Основы патентных правоотношений. Условия патентоспособности.
16. Объекты изобретения, связанные с электронно-вычислительной техникой и информационными технологиями. Авторы изобретений и патентообладатели. Механизм патентования. Защита прав патентообладателей и авторов.
17. Особенности договорных отношений в области информационной безопасности. Правовое регулирование взаимоотношений администрации и персонала в области обеспечения информационной безопасности. Особенности трудовых отношений.
18. Компьютерные правонарушения. Преступления в сфере компьютерной информации. Признаки и элементы состава преступления. Административная ответственность за преступления в информационной сфере.
19. Международное законодательство в области защиты информации. Правовой режим участия в международном обмене. Субъекты и объекты международного информационного обмена.
20. Национальные законодательства о компьютерных правонарушениях и защите информации.
21. Международное сотрудничество в области борьбы с компьютерной преступностью.
22. Положения ГОСТ Р ИСО/МЭК 18044-2007г., «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности», имеющие значение для расследования инцидентов компьютерной безопасности.
23. Положения ГОСТ Р ИСО/МЭК 56824-2015 «Интеллектуальная собственность. Использование охраняемых результатов интеллектуальной деятельности в сети Интернет», имеющие значение для защиты интеллектуальной собственности российских государственных и коммерческих структур при ее попадании в Интернет.
24. Основные положения федерального закона от 26 июля 2017 года №187 – ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» для укрепления национальной системы защиты критической информационной инфраструктуры страны.

Требования к выполнению заданий, шкалы и критерии оценивания

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

Для оценивания результатов обучения на зачете используется - зачтено, не зачтено Соотношение показателей, критериев и шкалы оценивания результатов обучения.

Показатель сформированности компетенции	Шкала и критерии оценивания уровня освоения компетенции	
	Зачтено	Не зачтено
Знает: международные и отечественные нормативно-правовые акты, стандарты и правила в области информационных технологий и информационной безопасности.	1. Сформированные знания 2. Сформированные знания, но содержащие отдельные пробелы 3. Неполные знания.	Фрагментарные знания или их отсутствие.
Владеет: знаниями международных и отечественных нормативно-правовых актов, стандартов	1. Сформированные знания 2. Сформированные знания, но содержащие отдельные пробелы	Неполные знания. / Фрагментарные знания или их отсутствие.

и правил в области информационных технологий и информационной безопасности		

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

ПК-3. Способен участвовать в работах по проектированию систем защиты информации в компьютерных системах и сетях при решении профессиональных, исследовательских и прикладных задач.

1. Хищение информации – это
   1. ***Несанкционированное копирование информации***
   2. Утрата информации
   3. Блокирование информации
   4. Искажение информации
   5. Продажа информации
2. Документированная информация, доступ к которой ограничивается в соответствии с законодательством российской федерации - это:
   1. ***Конфиденциальная информация***
   2. Факс
   3. Личный дневник
   4. Законы РФ
3. Обеспечение информационной безопасности есть обеспечение…
   1. Независимости информации
   2. Изменения информации
   3. Копирования информации
   4. ***Сохранности информации***
   5. Преобразования информации
4. Степени секретности информации, составляющей гостайну:
   а. особо секретно;
   б. конфиденциально;
   в. строго конфиденциально;
   г. совершенно конфиденциально;
   д. секретно;
   е. особой важности.
5. Не подлежат отнесению к государственной тайне сведения:
   а. о состоянии обороноспособности объектов жизнеобеспечения населения;
   б. о фактах нарушения прав и свобод человека и гражданина;
   в. о размерах золотого запаса и государственных валютных резервах Российской Федерации;
   г. о состоянии и средствах защиты государственной тайны;
   д. о состоянии здоровья высших должностных лиц Российской Федерации;
6. К видам информации с ограниченным доступом не относятся:
   а. коммерческая тайна;
   б. государственная тайна;
   в. сведения для служебного пользования;
   г. персональные данные;
   д. запрещенные к распространению сведения;
   е. нотариальная тайна.
7. Контроль над выполнением требований в сфере защиты персональных данных выполняют:
   а)ФСБ РФ;
   б) ФСТЭК России и Роскомнадзор;
   в) все перечисленные организации.

8. За несоблюдение положений закона 152-ФЗ «О персональных данных» предусматривается:
а) гражданская, уголовная, административная ответственность; б) дисциплинарная и другие виды ответственности;
в) все перечисленные виды ответственности.
9. Субъект персональных данных:
а) имеет право на доступ к своим персональным данным во всех случаях;
б) не имеет право на доступ к своим персональным данным;
в) имеет право на доступ к своим персональным данным за исключением случаев, предусмотренных законом.
10. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, при обработке персональных данных в государственных информационных системах осуществляются:
а) ФСТЭК России и ФСБ России;
б) ФСТЭК России и органами Роскомнадзора;
в) ФСБ России и органами Роскомнадзора.
11. Какой нормативный акт является основным в сфере регулирования электронной подписи:
а) федеральный закон №1-ФЗ от 10.01.2002 «Об электронной цифровой подписи»;
б) федеральный закон №63-ФЗ от 06.04.2011 «Об электронной подписи»;
в) постановление Правительства Российской Федерации № 111 от 9 февраля 2012 г. «Об электронной подписи, используемой органами исполнительной власти и органами местногосамоуправления при организации электронного взаимодействия между собой».

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).