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

УТВЕРЖДАЮ

Заведующий кафедрой
Программного обеспечения и администрирования информационных систем
_____ *Артемов М.А.*
02.04.2024г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.О.32 Организация защиты информации

1. Код и наименование направления подготовки/специальности: 09.03.03 Прикладная информатика.

2. Профиль подготовки/специализация: прикладная информатика в юриспруденции.

3. Квалификация выпускника: бакалавриат.

4. Форма обучения: очная.

5. Кафедра, отвечающая за реализацию дисциплины: кафедра программного обеспечения и администрирования информационных систем.

6. Составители программы: Железняк В.П., к.т.н., доцент.

7. Рекомендована: НМС факультета ПММ, протокол №5 от 22.03.2024

---

8. Учебный год: 2024-2025 **Семестр(ы)/Триместр(ы):** 7, 8

9. **Цели и задачи учебной дисциплины:** сформировать представление об организационных аспектах информационной безопасности и защиты информации, категориях защищаемой информации, объектах защиты, уязвимостях и угрозах безопасности информации, мерах защиты информации.

10. Место учебной дисциплины в структуре ООП: дисциплина относится к Б1.Б.21.

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

Код	Наименование компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1 ОПК-3.2	Применяет типовые математические модели на практике. Модифицирует выбранную математическую модель при разработке программных продуктов	Знать: теоретические и практические основы информационной безопасности и защиты информации, терминологию предметной области. Уметь: проводить классификацию (категорирование) информации. Определять защищаемую информацию и объекты защиты. Определять угрозы безопасности информации. Определять меры защиты информации. Владеть: знаниями о порядке категорирования информации и классификации различных типов информационных систем, порядке определения угроз

Код	Наименование компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
				безопасности информации, порядке разработки системы защиты информации

12. Объем дисциплины в зачетных единицах/час: 4/144.

Форма промежуточной аттестации: зачет, дифференцированный зачет.

13. Виды учебной работы

Вид учебной работы		Трудоемкость		
		Всего	По семестрам	
			Семестр 7	Семестр 8
Аудиторные занятия				
в том числе:	лекции	48	32	16
	практические	0	0	0
	лабораторные	16	16	0
Самостоятельная работа		80	42	38
в том числе: курсовая работа (проект)				
Форма промежуточной аттестации *(зачет – _час.)*		22,5	11,25	11,25
Итого:		144	90	54

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1.	Введение в информационную безопасность и защиту информации	Понятие информации. Разделение информации в зависимости от категории доступа к ней. Понятие обладателя информации. Права обладателя информации. Понятие обработки информации. Понятие защиты информации. Меры защиты информации. Обеспечиваемые характеристики безопасности. Понятие конфиденциальности. Понятие доступности. Понятие целостности. Понятие системы защиты информации. Понятие информационной безопасности	https://edu.vsu.ru/enrol/index.php?id=6110
2.	Классификация (категорирование) информации. Определение защищаемой информации	Понятие категорирования защищаемой информации. Существующие категории информации с ограниченным доступом. Понятие	https://edu.vsu.ru/enrol/index.php?id=6110

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
		государственной тайны. Степени секретности сведений, составляющих государственную тайну. Перечень сведений конфиденциального характера, утвержденный Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»	
3.	Персональные данные. Особенности обработки	Понятие персональных данных. Понятие оператора персональных данных. Категории персональных данных. Специальные категории персональных данных. Понятие биометрических персональных данных. Понятие персональных данных, разрешенных субъектом персональных данных для распространения. Понятие обработки персональных данных. Виды обработки персональных данных. Понятие автоматизированной обработки персональных данных. Принципы обработки персональных данных. Условия обработки персональных данных. Виды согласий на обработку персональных данных. Поручение на обработку персональных данных	https://edu.vsu.ru/enrol/index.php?id=6110

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
4.	Меры, направленные на обеспечение выполнения обязанностей, возложенных на оператора персональных данных	Состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами	https://edu.vsu.ru/enrol/index.php?id=6110
5.	Коммерческая тайна	Понятие коммерческой тайны. Понятие информации, составляющей коммерческую тайну. Условия отнесения информации к коммерческой тайне. Понятие обладателя информации, составляющей коммерческую тайну. Права обладателя информации, составляющей коммерческую тайну. Мероприятия по установлению режима коммерческой тайны. Обязанности работника по охране конфиденциальности информации, составляющей коммерческую тайну	https://edu.vsu.ru/enrol/index.php?id=6110
6.	Объекты защиты информации	Понятие объекта защиты информации. Что может относиться к объектам защиты информации. Понятие информационной системы. Понятие государственной	https://edu.vsu.ru/enrol/index.php?id=6110

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
		информационной системы. Понятие муниципальной информационной системы. Понятие информационной системы персональных данных. Основные критерии, характеризующие информационные системы с точки зрения их исходной защищенности. Понятие объекта информатизации	
7.	Классификация по требованиям защиты информации	Порядок классификации государственных информационных систем. Определяющие признаки для определения класса защищенности информационной системы. Понятие уровня значимости информации, его определение Порядок определения уровня защищенности персональных данных при их обработке в информационной системе. Определяющие признаки для определения уровня защищенности персональных данных при их обработке в информационной системе. Понятие недекларированных возможностей. Типы актуальных угроз безопасности персональных данных	https://edu.vsu.ru/enrol/index.php?id=6110

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
8.	Угрозы безопасности информации	Понятие угрозы безопасности информации. Цель определения угроз безопасности информации. Источники угроз безопасности информации. Понятие и виды технических каналов утечки информации	https://edu.vsu.ru/enrol/index.php?id=6110
9.	Нарушители безопасности информации	Понятие нарушителя безопасности информации. Типы, виды нарушителей безопасности информации. Цели (мотивации) реализации нарушителями угроз безопасности информации. Определение потенциала нарушителя по реализации угроз безопасности информации	https://edu.vsu.ru/enrol/index.php?id=6110
10.	Система защиты информации	Понятие системы защиты информации. Меры защиты информации. Виды средств защиты информации. Сертификация средств защиты информации	https://edu.vsu.ru/enrol/index.php?id=6110

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1.	Введение в информационную безопасность и защиту информации	4	0	0	4	8
2.	Классификация (категорирование) информации. Определение защищаемой информации	6	0	2	10	18
3.	Персональные данные. Особенности обработки	6	0	2	6	14
4.	Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных Федеральным законом «О персональных данных	4	0	2	6	12
5.	Коммерческая тайна	2	0	0	4	6
6.	Объекты защиты информации	6	0	2	6	14
7.	Классификация по требованиям защиты информации	4	0	2	6	12
8.	Угрозы безопасности информации, их источники	4	0	2	14	20
9.	Нарушители безопасности информации	4	0	2	10	16
10.	Система защиты информации	8	0	2	14	24

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
		48	0	16	80	144

14. Методические указания для обучающихся по освоению дисциплины
работа с конспектами лекций, презентационным материалом.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины
а) основная литература:

№ п/п	Источник
1.	Основы информационной безопасности : учебное пособие / С.А. Нестеров. — Изд. 4-е, стер. — Санкт-Петербург ; Москва ; Краснодар : Лань, 2018 .— 321 с. : ил., табл. — (Учебники для вузов. Специальная литература) (Библиотека высшей школы). — Библиогр.: с. 319-321

б) дополнительная литература:

№ п/п	Источник
1.	Защита информации : учебное пособие для бакалавриата и магистратуры : [для студ. вузов, обучающихся по инженер.-техн. направлениям] / А.А. Внуков ; Национальный исслед. ун-т "Высшая школа экономики" .— 2-е изд., испр. и доп. — Москва : Юрайт, 2018. — 239, [1] с. : ил., табл. — (Бакалавр и магистр. Академический курс). — Библиогр.: с. 231-232
2.	Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов : [для студ. вузов, обучающихся по инженер.-техн. направлениям] / О.В. Казарин, А.С. Забабурин .— Москва : Юрайт, 2018 .— 311, [1] с. : ил., табл. — (Специалист) .— Библиогр. в конце гл. Организационно-правовое и методическое обеспечение информационной безопасности : учебное пособие / Н. С. Кармановский, О. В. Михайличенко, Н. Н. Прохожев. — Санкт-Петербург : НИУ ИТМО, 2016. — 168 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/91449. — Режим доступа: для авториз. пользователей
3.	Организационное и правовое обеспечение информационной безопасности : учебное пособие / Г. П. Жигулин. — Санкт-Петербург : НИУ ИТМО, 2014. — 173 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/70952. — Режим доступа: для авториз. пользователей
4.	Защита персональных данных : учебное пособие / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова. – Уфа : БашГУ, 2020. – 120 с. – ISBN 978-5-7477-5228-3. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/179914. – Режим доступа: для авториз. пользователей

№ п/п	Источник
5.	Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных : учебное пособие / Е. Г. Воробьев. – 3-е изд., перераб. – Санкт-Петербург : Интермедия, 2017. – 432 с. – ISBN 978-5-4383-0120-2. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/161356. – Режим доступа: для авториз. пользователей

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

№ п/п	Источник
1.	Электронный каталог Научной библиотеки Воронежского государственного университета. – URL: https://lib.vsu.ru
2.	Образовательный портал «Электронный университет ВГУ». – URL: https://edu.vsu.ru
3.	Информационно-правовая система «Законодательство России» // Официальный интернет-портал правовой информации – URL: http://pravo.gov.ru
4.	Банк данных угроз безопасности информации – URL: https://bdu.fstec.ru

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1.	Информационная безопасность : учебник и практикум для академического бакалавриата / С.А. Нестеров ; С.-Петерб. политехн. ун-т Петра Великого .— Москва : Юрайт, 2018 .— 321 с. : ил., табл. — (Университеты России) .— Библиогр.: с. 319-321

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение: образовательный портал «Электронный университет ВГУ». – URL: https://edu.vsu.ru.

18. Материально-техническое обеспечение дисциплины: лабораторный класс с проектором (ауд. 226, ауд. 227): компьютеры с доступом к сети «Интернет», операционная система, интернет-браузер, пакет офисного программного обеспечения, антивирусное программное обеспечение.

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.	1-10	ОПК-3	ОПК-3.1, ОПК-3.2	Опрос, обсуждение, выполнение практических заданий
Промежуточная аттестация форма контроля – зачет, экзамен				Перечень вопросов. Практическое задание

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: практико-ориентированные задания, тестовые задания.

Вопросы:

1. Понятие информации.
2. Разделение информации в зависимости от категории доступа к ней.
3. Понятие обладателя информации.
4. Права обладателя информации.
5. Понятие обработки информации.
6. Понятие защиты информации.
7. Меры защиты информации.
8. Понятие правовой защиты информации.
9. Понятие защита информации организационной.
10. Понятие технической защиты информации.
11. Понятие криптографической защиты информации.
12. Обеспечиваемые характеристики безопасности.
13. Понятие конфиденциальности.
14. Понятие доступности.
15. Понятие целостности.
16. Понятие системы защиты информации.
17. Понятие информационной безопасности.
18. Понятие категорирования защищаемой информации.
19. Существующие категории информации с ограниченным доступом.
20. Понятие государственной тайны.
21. Степени секретности сведений, составляющих государственную тайну.
22. Перечень сведений конфиденциального характера.
23. Понятие персональных данных.
24. Понятие оператора персональных данных.
25. Категории персональных данных.
26. Специальные категории персональных данных.
27. Понятие биометрических персональных данных.
28. Понятие персональных данных, разрешенных субъектом персональных данных для распространения.
29. Понятие распространения персональных данных.
30. Понятие предоставления персональных данных.
31. Понятие обработки персональных данных.
32. Виды обработки персональных данных.
33. Понятие автоматизированной обработки персональных данных.
34. Основная суть принципа обработки персональных данных: обработка персональных данных должна осуществляться на законной и справедливой основе.

35. Основная суть принципа обработки персональных данных: обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей.

3. Основная суть принципа обработки персональных данных: не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

4. Основная суть принципа обработки персональных данных: обработке подлежат только персональные данные, которые отвечают целям их обработки.

5. Основная суть принципа обработки персональных данных: содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки.

6. Основная суть принципа обработки персональных данных: при обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных.

7. Основная суть принципа обработки персональных данных: хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных.

36. Виды согласий на обработку персональных данных.

37. Требования к содержанию согласия на обработку персональных данных в письменной форме.

38. Требования к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

39. Основная суть условия обработки персональных данных: обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей.

40. Основная суть условия обработки персональных данных: обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах.

41. Основная суть условия обработки персональных данных: обработка персональных данных необходима для исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве.

42. Основная суть условия обработки персональных данных: обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг.

43. Основная суть условия обработки персональных данных: обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем.

44. Основная суть условия обработки персональных данных: обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно

важных интересов субъекта персональных данных, если получение согласия *субъекта персональных данных* невозможно.

45. Основная суть условия обработки персональных данных: обработка персональных данных необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы субъекта персональных данных.

46. Основная суть условия обработки персональных данных: обработка персональных данных осуществляется в статистических или иных исследовательских целях, за исключением целей продвижения товаров, работ, услуг на рынке, а также политической агитации, при условии обязательного обезличивания персональных данных.

47. Основная суть условия обработки персональных данных: осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

48. Требования к поручению на обработку персональных данных.

49. Основное содержание меры: назначение ответственного за организацию обработки персональных данных.

50. Основное содержание меры: издание оператором документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства, устранение последствий таких нарушений.

51. Основное содержание меры: осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора.

52. Основное содержание меры: ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

53. Основное содержание меры: применение правовых, организационных и технических мер по обеспечению безопасности персональных данных при их обработке.

54. Понятие несанкционированного доступа к информации.

55. Понятие коммерческой тайны.

56. Понятие информации, составляющей коммерческую тайну.

57. Условия отнесения информации к коммерческой тайне.

58. Понятие обладателя информации, составляющей коммерческую тайну.

59. Права обладателя информации, составляющей коммерческую тайну.

60. Мероприятия по установлению режима коммерческой тайны.

61. Обязанности работника по охране конфиденциальности информации, составляющей коммерческую тайну.

62. Понятие объекта защиты информации.

63. Понятие информационной системы.

64. Понятие государственной информационной системы.

65. Понятие муниципальной информационной системы.

66. Понятие информационной системы персональных данных.

67. Понятие объекта информатизации.

68. Определяющие признаки для определения класса защищенности информационной системы.

69. Уровень значимости информации.

70. Определяющие признаки для определения уровня защищенности персональных данных при их обработке в информационной системе.

71. Понятие недекларированных возможностей.

72. Понятие угрозы безопасности информации.

73. Цель определения угроз безопасности информации.

74. Источники угроз безопасности информации.

75. Понятие и виды технических каналов утечки информации.

76. Понятие нарушителя безопасности информации.

77. Типы, виды нарушителей безопасности информации.

78. Цели (мотивации) реализации нарушителями угроз безопасности информации;

79. Определение потенциала нарушителя по реализации угроз безопасности информации.

80. Понятие системы защиты информации.

81. Меры защиты информации по идентификации и аутентификации субъектов доступа и объектов доступа с примерами.

82. Меры защиты информации по управлению доступом субъектов доступа к объектам доступа с примерами.

83. Меры защиты информации по ограничению программной среды с примерами.

84. Меры защиты информации по защите машинных носителей информации с примерами.

85. Меры защиты информации по регистрации событий безопасности с примерами.

86. Меры защиты информации по антивирусной защите с примерами.

87. Меры защиты информации по обнаружению (предотвращению) вторжений с примерами.

88. Меры защиты информации по контролю (анализу) защищенности информации с примерами.

89. Меры защиты информации по обеспечению целостности информационной системы и информации с примерами.

90. Меры защиты информации по обеспечению доступности информации с примерами.

91. Меры защиты информации по защите среды виртуализации с примерами.

92. Меры защиты информации по защите технических средств с примерами.

93. Меры защиты информации по защите информационной системы, ее средств, систем связи и передачи данных с примерами.

20.2. Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: лабораторные работы.

Перечень тем:

лабораторная работа с категориями информации ограниченного доступа;

лабораторная работа с реестром операторов персональных данных;

лабораторная работа с уязвимостями программного обеспечения.