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

УТВЕРЖДАЮ
Заведующий кафедрой
уравнений в частных производных
и теории вероятностей
А.В. Глушко
16.04.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.ДВ.03.02 Безопасность программного обеспечения

1. Код и наименование специальности: 0 1.04.04 Прикладная математика

2. Профиль подготовки: Применение математических методов к решению инженерных и экономических задач

3. Квалификация выпускника: магистр

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: кафедра уравнений в частных производных и теории вероятностей

6. Составители программы: Ткачева Светлана Анатольевна, кандидат физико-математических наук, доцент

7. Рекомендована: Научно-методическим советом математического факультета

Протокол № 0500-03 от 28.03.24

8. Учебный год: 2025/2026 **Семестр:** 4

9. **Цели и задачи учебной дисциплины**

Цели освоения учебной дисциплины:

- формирование знаний о безопасности программного обеспечения,
- приобретение практических навыков анализа безопасности программного обеспечения.

Задачи учебной дисциплины:

- освоение методов анализа и оценки основных направлений обеспечения безопасности программного обеспечения.

10. Место учебной дисциплины в структуре ООП: Блок 1, вариативной части обучения, дисциплина по выбору.

Для успешного освоения дисциплины необходимы знания и умения, приобретенные в результате обучения по предшествующим дисциплинам: «Математические методы и модели теории кодирования и криптологии и разработка на их основе программного обеспечения информационно-коммуникационных технологий», «Математические методы в актуарных расчетах».

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 руководить проектами по созданию и эксплуатации программного обеспечения для решения инженерных и экономических задач	ПК-2.1	Знает методы и средства разработки программного обеспечения	Знать: методы и средства разработки программного обеспечения Уметь: применять разработанное программное обеспечение Владеть: навыками работы с программным обеспечением, разрабатывать и внедрять новые программные продукты
		ПК-2.3	Владеет методами решения прикладных задач, используя современное прикладное программное обеспечение	Знать: методы решения прикладных задач, с использованием современного программного обеспечения Уметь: выбирать подходящий метод решения конкретной прикладной задачи с использованием современного программного обеспечения Владеть: навыками и инструментами решения практических задач с использованием прикладного программного обеспечения

12. Объем дисциплины в зачетных единицах/час. — __2__/__72___.

Форма промежуточной аттестации зачет

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоемкость		
	Всего	По семестрам	
		8 семестр	
Контактная работа	20	20	

в том числе:	лекции	10	10	
	практические	-	-	
	лабораторные	10	10	
	курсовая работа	-	-	
	контрольные работы	1	1	
Самостоятельная работа		52	52	
Промежуточная аттестация		-	-	
Итого:		**72**	**72**	

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК*
1. Лекции			
1.1	Защита программного обеспечения компьютерных систем	Угрозы безопасности программного обеспечения и примеры их реализации в современном компьютерном мире	-
		Жизненный цикл программного обеспечения компьютерных систем. Технологическая и эксплуатационная безопасность программ. Модель угроз и принципы обеспечения безопасности ПО	
1.2	Обеспечение технологической безопасности программного обеспечения	Формальные методы доказательства правильности программ и их спецификаций. Методы и средства анализа безопасности программного обеспечения. Методы обеспечения надежности программ для контроля их технологической безопасности	-
		Методы создания алгоритмически безопасных процедур. Подходы к защите разрабатываемых программ от автоматической генерации инструментальными средствами программных закладок. Методы идентификации программ и их характеристик	
1.3	Обеспечение эксплуатационной безопасности программного обеспечения	Методы и средства защиты программ от компьютерных вирусов. Методы защиты программного обеспечения от внедрения на этапе его эксплуатации и сопровождения программных закладок	-
		Методы и средства обеспечения целостности и достоверности используемого программного кода. Основные подходы к защите программ от несанкционированного копирования	
1.4	Правовая и организационная поддержка процессов разработки и применения программного обеспечения	Стандарты и другие нормативные документы, регламентирующие защищенность программного обеспечения и обрабатываемой информации. Сертификационные испытания программных средств, безопасность программного обеспечения и человеческий фактор, психология программирования	-
1.5	Безопасность программного обеспечения и человеческий фактор.	Психология программирования, человеческий фактор. Международные нормативные документы, связанные с проблематикой обеспечения безопасности программного обеспечения	-
3. Лабораторные занятия			

3.1	Защита программного обеспечения компьютерных систем	Угрозы безопасности программного обеспечения и примеры их реализации в современном компьютерном мире	-
		Жизненный цикл программного обеспечения компьютерных систем. Технологическая и эксплуатационная безопасность программ. Модель угоз и принципы обеспечения безопасности ПО. Перечень типовых дефектов разработки, влияющих на безопасность ПО, и программных закладок, замаскированных под дефекты разработки	
3.2	Обеспечение технологической безопасности программного обеспечения	Формальные методы доказательства правильности программ и их спецификаций. Методы и средства анализа безопасности программного обеспечения. Методы обеспечения надежности программ для контроля их технологической безопасности	-
		Методы создания алгоритмически безопасных процедур. Подходы к защите разрабатываемых программ от автоматической генерации инструментальными средствами программных закладок. Методы идентификации программ и их характеристик. Характеристики программ с точки зрения влияния на их защищенность и результаты работы.	
3.3	Обеспечение эксплуатационной безопасности программного обеспечения	Методы и средства защиты программ от компьютерных вирусов. Методы защиты программного обеспечения от внедрения на этапе его эксплуатации и сопровождения программных закладок	-
		Методы и средства обеспечения целостности и достоверности используемого программного кода. Основные подходы к защите программ от несанкционированного копирования.	
3.4	Правовая и организационная поддержка процессов разработки и применения программного обеспечения	Стандарты и другие нормативные документы, регламентирующие защищенность программного обеспечения и обрабатываемой информации. Сертификационные испытания программных средств, безопасность программного обеспечения и человеческий фактор, психология программирования	-
3.5	Безопасность программного обеспечения и человеческий фактор.	Психология программирования, человеческий фактор. Международные нормативные документы, связанные с проблематикой обеспечения безопасности программного обеспечения. Контрольная работа	-

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	Защита программного обеспечения компьютерных систем	2	-	2	10	14
2	Обеспечение технологической безопасности программного обеспечения	2	-	2	10	14
3	Обеспечение эксплуатационной безопасности программного обеспечения	2	-	2	12	16

4	Правовая и организационная поддержка процессов разработки и применения программного обеспечения	2	-	2	10	14
5	Безопасность программного обеспечения и человеческий фактор.	2	-	2	10	14
	Итого:	10	-	10	52	72

14. Методические указания для обучающихся по освоению дисциплины:

В процессе преподавания дисциплины используются такие виды учебной работы, как лекции, лабораторные занятия, а также различные виды самостоятельной работы обучающихся, на которую отводится 52 часа.

Самостоятельная учебная деятельность студентов по дисциплине «Безопасность программного обеспечения» предполагает выполнение следующих заданий:

1) самостоятельное изучение учебных материалов по разделам 1-5 с использованием основной и дополнительной литературы, информационно-справочных и поисковых систем;

2) подготовку к текущим аттестациям: выполнение лабораторных заданий, самостоятельное освоение понятийного аппарата по каждой теме.

3) по темам 1-5 обучающиеся сдают реферат. Примерные темы рефератов:

1. Методы создания алгоритмически безопасных процедур
2. Подходы к защите разрабатываемых программ от автоматической генерации инструментальными средствами программных закладок
3. Методы идентификации программ и их характеристик
4. Методы и средства защиты программ от компьютерных вирусов
5. Методы защиты программного обеспечения от внедрения на этапе его эксплуатации и сопровождения программных закладок .
6. Методы и средства обеспечения целостности и достоверности используемого программного кода
7. Основные подходы к защите программ от несанкционированного копирования .
8. Стандарты и другие нормативные документы, регламентирующие защищенность программного обеспечения и обрабатываемой информации
9. Сертификационные испытания программных средств.
10. Безопасность программного обеспечения и человеческий фактор.

На лекциях рассказывается теоретический материал, на практических занятиях решаются задачи и выполняются практические задания по теоретическому материалу, прочитанному на лекциях.

При изучении курса «Безопасность программного обеспечения» обучающимся следует внимательно слушать и конспектировать материал, излагаемый на аудиторных занятиях. Для его понимания и качественного усвоения рекомендуется следующая последовательность действий.

1. После каждой лекции обучающимся рекомендуется подробно разобрать прочитанный теоретический материал, выучить все определения и формулировки, разобрать примеры и задания, рассмотренные на лекции. Перед следующей лекций обязательно повторить материал предыдущей лекции.

2. Перед практическим занятием обязательно повторить лекционный материал. После практического занятия еще раз разобрать разобранные на этом занятии задания, после чего приступить к выполнению домашнего задания. Если при выполнении заданий

возникнут вопросы, обязательно задать на следующем практическом занятии или в присутственный час преподавателю.

3. Выбрать время для работы с литературой по дисциплине в библиотеке.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и ресурсами сети Internet, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся заинтересованное отношение к конкретной проблеме.

Виды самостоятельной работы: конспектирование учебной и научной литературы; проработка учебного материала (по конспектам лекций, учебной и научной литературе); работа в электронной библиотечной системе; работа с информационными справочными системами, выполнение домашних заданий (практических и теоретических); выполнение контрольной работы; подготовка к практическим занятиям.

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

а) основная литература:

№ п/п	Источник
1	Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие / А. В. Душкин, О. М. Барсуков, Е. В. Кравцов, К. В. Славнов ; под редакцией А. В. Душкина. — Москва : Горячая линия-Телеком, 2018. — 248 с. — ISBN 978-5-9912-0470-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111053
2	Шилер, А. В. Обеспечение информационной безопасности корпоративных информационных сетей на базе программного комплекса SecureTower : учебно-методическое пособие / А. В. Шилер, А. А. Елизаров, Е. А. Степанова. — Омск : ОмГУПС, 2020. — 23 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165730

б) дополнительная литература:

№ п/п	Источник
1	Булычев, Г. Г. Программно-аппаратные средства обеспечения информационной безопасности : методические указания / Г. Г. Булычев. — Москва : РТУ МИРЭА, 2020 — Часть 2 — 2020. — 46 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163812
2	Смирнов, А. А. Прикладное программное обеспечение : учебное пособие : [16+] / А. А. Смирнов. – Москва ; Берлин : Директ-Медиа, 2017. – 358 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=457616

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

№ п/п	Ресурс
1	*http://www.lib.vsu.ru - электронный каталог ЗНБ ВГУ*
2	*http://www.kuchp.ru – электронный сайт кафедры уравнений в частных производных и теории вероятностей, на котором размещены методические издания*
3	https://edu.vsu.ru/ – *образовательный портал «Электронный университет ВГУ»/LMC Moodle*

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Андреев, А. Е. Адаптивные технологии разработки программного обеспечения : учебное пособие / А. Е. Андреев, С. И. Кирносенко. — Волгоград : ВолгГТУ, 2015. — 96 с. — ISBN 978-5-9948-1979-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157223
2	Казарин О.В. Безопасность программного обеспечения компьютерных систем. / О.В. Казарин - М.: МГУЛ, 2003. - 212 с. http://window.edu.ru/resource/846/23846/files/kazarin.pdf
3	Положение об организации самостоятельной работы обучающихся в Воронежском государственном университете.

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

При реализации дисциплины используются следующие образовательные технологии: логическое построение дисциплины, установление межпредметных связей, обозначение теоретического и практического компонентов в учебном материале, актуализация личного и учебно-профессионального опыта обучающихся, включение элементов дистанционных образовательных технологий.

В практической части курса используется стандартное современное программное обеспечение персонального компьютера.

В части освоения материала лекционных и лабораторных занятий, самостоятельной работы по отдельным разделам дисциплины, прохождения текущей и промежуточной аттестации может применяться электронное обучение и дистанционные образовательные технологии, размещенные на портале «Электронный университет ВГУ».

18. Материально-техническое обеспечение дисциплины:

Для проведения лекционных и лабораторных занятий используются учебные аудитории.

Для самостоятельной работы используется класс с компьютерной техникой.

Компьютерный класс: специализированная мебель, маркерная доска, персональные компьютеры

В самостоятельной работе обучающиеся используют ресурсы Зональной научной библиотеки ВГУ (электронный каталог: http://www.lib.vsu.ru).

19. Фонд оценочных средств:

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.	Защита программного обеспечения компьютерных систем	ПК-2	ПК-2.1	Контрольная работа 1
2.	Обеспечение технологической безопасности программного обеспечения	ПК-2	ПК-2.1	Контрольная работа, тестовые задания
3.	Обеспечение эксплуатационной безопасности программного обеспечения	ПК-2	ПК-2.1	Контрольная работа, тестовые задания
4.	Правовая и организационная поддержка процессов разработки и применения программного обеспечения	ПК-2	ПК-2.1	Контрольная работа, тестовые задания
5.	Безопасность	ПК-2	ПК-2.1	Контрольная работа, тестовые задания

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
	программного обеспечения и человеческий фактор.			
Промежуточная аттестация форма контроля – _зачет_____				Перечень вопросов к зачету

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: контрольная работа, тестовые задания.

Перечень тестовых заданий для контрольной работы:

Вариант №1

1. Свойства информации в форме сообщения:

(укажите правильный вариант)

идеальность субъективность информационная
неуничтожаемость динамичность материальность накапливаемость

2. Свойства информации в форме сведений: (укажите правильный вариант)

материальность измеримость сложность проблемная ориентированность накапливаемость

3. Информационная сфера – это … , … , … , … .

5. Общие методы обеспечения информационной безопасности

… … …

6. Информация – наиболее ценный … современного общества.

7. К какому классу информационных ресурсов относятся автоматизированные рабочие места проектировщиков?

Документы Персонал Организационные единицы Промышленные образцы Научный инструментарий

8. Поставьте в порядке важности национальные интересы:

Информационное обеспечение государственной политики Российской Федерации. Развитие современных информационных технологий отечественной индустрии информации. Соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею. Защита информационных ресурсов от несанкционированного доступа

9. Допишите различные подходы к понятию информации:

информация … информация … … информация

10. Перечислите составляющие национальной безопасности:

Пример варианта контрольной работы 1:

Вариант 1

1. Какой метод обеспечения информационной безопасности отсутствует в перечне :

ОрганизационныйПравовой Технический
Экономический Идеологический

2. Совокупность информации, информационной инфраструктуры, субъектов и системы регулирования общественных отношений являются составляющими частями … … .

3. Автономная информация – информация , существующая … от какого-либо субъекта.

4. Информационная сфера – являясь системообразующим фактором жизни общества, активно влияет на сосояние … , … , … и др. составляющих безопасности Российской Федерации.

5. Информация взаимодействия - … одного субъекта на другого, имеющее целью …, моделей внешней среды двух субъектов или коллектива.

6. Информация воздействия - … знания, … модели окружающего мира.

7. Информационная безопасность - … защищенности национальных интересов РФ в информационной сфере, определяющихся совокупностью … интересов личности, общества и государства.

8. Составляющие национальной безопасности:

соблюдение … Российской Федерации. Правовое … всех участников процесса информационного взаимодействия. Соблюдение … прав и свобод человека и гражданина в области получения информации и пользования ею.

d. Приоритетное … отечественных современных информационных и телекоммуникационных технологий

9. Общая схема национальной безопасности:

Формулировка … Формирование перчня … Оценка … и … Разработка … Принятие …
10. Свойства информации в форме сообщения: (укажите правильный вариант)

a. идеальность c. динамичность информационная неуничтожаемость
b. субъективностьd. накапливаемостьизмеримость

Тестовые задания (коллоквиум)

Вариант №1

1. Информация – наиболее ценный … современного общества.

2. Поставьте в порядке важности национальные интересы:

Информационное обеспечение государственной политики Российской Федерации. Развитие современных ИТ , отечественной индустрии информации. Соблюдение конституционных прав и

свобод человека и гражданина в области получения информации и пользования ею. Защита информационных ресурсов от несанкционированного доступа

3. Допишите различные подходы к понятию информации:

информация …
информация …
информация …

4. Составляющие национальной безопасности:

5. К какому классу информационных ресурсов относятся автоматизированные рабочие места проектировщиков?

Документы Персонал Организационные единицы Промышленные образцы Научный инструментарий

6. Перечислите информационное оружие:

… … средства … генераторы средства … средства …

7. Война, есть продолжение … другими, насильственными средствами.

8. В Концепции национальной безопасности введено понятие национальных интересов, как совокупности сбалансированных интересов … , … , … .

9. Информационная сфера – это … , … , … , … .

10. Первая классификация национальных интересов:…

11. Общие методы обеспечения информационной безопасности

12. Свойства информации в форме сообщения:(укажите правильный вариант)

субъективность информационная
неуничтожаемость динамичность материальность накапливаемость

13. Общие методы обеспечения национальной безопасности:

… … …

14. Основные объекты воздействия в информационной войне?

… b. … c. … d. … e. …

15. Свойства информации в форме сведений: (укажите правильный вариант)

материальность измеримость сложность проблемная ориентированность накапливаемость

16. Информационные угрозы:
а) нарушение целостности информации, прерывание, модификация и кража информации, разрушение данных,
б) несанкционированная передача информации, разрушение данных, в) применение вирусов и других средств воздействия на технические и программные средства,
г) перехват информации при передаче.

17. Законные методы получения информации:

а) изучение рекламы конкурентов, похищение образцов,
б) сбор информации в СМИ, изучение рекламы, продукции и фирменных магазинов,
в) получение информации с помощью сотрудников и технических средств, г) изучение договоров.

18. Предотвращение компьютерных преступлений:

а) слежка за персоналом,
б) специальное ПО для негласного контроля за работой сотрудников на ПК,
в) использование «лояльных» хакеров,
г) все перечисленное.

19. К объектам кадровой безопасности не относятся:
а) соискатели вакантной должности экономического субъекта;
б) руководители экономического субъекта;
в) сотрудники экономического субъекта;
г) государственная инспекция труда;
д) сотрудники экономического субъекта, уволенные по собственному желанию.

20. Целью функционирования системы обеспечения технико-технологической безопасности организации являются:
а) предупреждение и нивелирование угроз ресурсам организации;
б) предупреждение и нивелирование угроз финансовым интересам организации;
в) предупреждение и нивелирование угроз имущественному потенциалу и технологическому процессу.

Описание технологии проведения

В ходе контрольной работы 1 обучающемуся выдается КИМ с 10 тестовыми заданиями. Ограничение по времени – 15 минут. Во время контрольной работы не разрешено пользоваться никакими справочными материалами.

При проведении коллоквиума обучающемуся выдается КИМ с 20 тестовыми заданиями. Ограничение по времени – 30 минут. Во время коллоквиума не разрешено пользоваться никакими справочными материалами.

Текущая аттестация по дисциплине с применением дистанционных образовательных технологий может проводиться на образовательном портале «Электронный университет ВГУ» (LMS Moodle, https://edu.vsu.ru/).

Требования к выполнению заданий (или шкалы и критерии оценивания). При текущем контроле уровень освоения учебной дисциплины и степень сформированности компетенции определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», которые формируются следующим образом:

Контрольная работа

Оценки	Критерии
Отлично	обучающийся правильно выполнил не менее 95% тестовых заданий контрольной работы.
Хорошо	обучающийся правильно выполнил не менее 75% тестовых заданий контрольной работы.
Удовлетворительно	Обучающийся правильно выполнил не менее 50% предложенных тестовых заданий.
Неудовлетворительно	Обучающийся правильно выполнил менее 50% предложенных заданий.

Тестовые задания(коллоквиум) (часть1, часть 2)

Оценки	Критерии
Отлично	обучающийся правильно выполнил не менее 95% тестовых заданий, представлено полное и правильное решение каждой из задач, сделаны обоснованные выводы.

Хорошо	обучающийся правильно выполнил не менее 75% тестовых заданий, решил все задачи, однако, представленные решения недостаточно обоснованы, либо в ходе решения задач обучающимся допущены несущественные ошибки (не более двух).
Удовлетворительно	Обучающийся правильно выполнил не менее 50% тестовых заданий, правильно решил не менее 50% задач.
Неудовлетворительно	Обучающийся правильно выполнил менее 50% тестовых заданий и/или решил менее 50% задач.

20.2. Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: выполнение заданий контрольной работы на оценку не ниже «удовлетворительно», ответы на тестовые задания собеседование по билетам к зачету.

Перечень вопросов к зачету:

1.Зачем и от кого нужно защищать программное обеспечение компьютерных систем

2. Угрозы безопасности программного обеспечения и примеры их реализации в современном компьютерном мире.

3. Базовые научные дисциплины, принятая аксиоматика и терминология.

4. Жизненный цикл программного обеспечения компьютерных систем.

5. Технологическая и эксплуатационная безопасность программ

6. Модель угроз и принципы обеспечения безопасности программного обеспечения

7. Формальные методы доказательства правильности программ и их спецификаций

8. Методы и средства анализа безопасности программного обеспечения

9. Методы обеспечения надежности программ для контроля их технологической безопасности

10. Методы создания алгоритмически безопасных процедур

11. Подходы к защите разрабатываемых программ от автоматической генерации инструментальными средствами программных закладок

12. Методы идентификации программ и их характеристик

13. Методы и средства защиты программ от компьютерных вирусов

14. Методы защиты программного обеспечения от внедрения на этапе его эксплуатации и сопровождения программных закладок .

15. Методы и средства обеспечения целостности и достоверности используемого программного кода

16. Основные подходы к защите программ от несанкционированного копирования .

17. Стандарты и другие нормативные документы, регламентирующие защищенность программного обеспечения и обрабатываемой информации

18. Сертификационные испытания программных средств.

19. Безопасность программного обеспечения и человеческий фактор.

20. Психология программирования.

Пример контрольно-измерительного материала(зачет):

Контрольно-измерительный материал №_1_

1. Методы и средства анализа безопасности программного обеспечения
2. Технологическая и эксплуатационная безопасность программ.
3. Основные подходы к защите программ от несанкционированного копирования.

Описание технологии проведения.

Промежуточная аттестация по дисциплине «Безопасность программного обеспечения»

проводится в форме зачета.

По решению кафедры оценки за экзамен могут быть выставлены по результатам текущей успеваемости обучающегося в течение семестра, но не ранее, чем на заключительном занятии. Для этого обучающемуся необходимо написать контрольную работу и ответить на тестовые задания на оценку не ниже «удовлетворительно», посетить не менее 80% занятий, активно работать на занятиях. При несогласии обучающегося, ему дается возможность пройти промежуточную аттестацию на общих основаниях.

Промежуточная аттестация, как правило, осуществляется в конце семестра.

Промежуточная аттестация по дисциплине с применением электронного обучения, дистанционных образовательных технологий (далее – ЭО, ДОТ) может проводиться на образовательном портале «Электронный университет ВГУ» (LMS Moodle, https://edu.vsu.ru/).

Обучающиеся, проходящие промежуточную аттестацию с применением ДОТ, должны располагать техническими средствами и программным обеспечением, позволяющим обеспечить процедуры аттестации. Обучающийся самостоятельно обеспечивает выполнение необходимых технических требований для проведения промежуточной аттестации с применением дистанционных образовательных технологий.

Идентификация личности обучающегося при прохождении промежуточной аттестации обеспечивается посредством использования каждым обучающимся индивидуального логина и пароля при входе в личный кабинет, размещенный в ЭИОС образовательной организации.

В ходе проведения аттестации обучающемуся необходимо ответить на вопросы КИМ, состоящего из двух вопросов, и дополнительные вопросы экзаменатора.

Результаты текущей аттестации обучающегося учитываются при проведении промежуточной аттестации следующим образом: обучающиеся, получившие хотя бы за одну контрольную работу оценку «не удовлетворительно» или не явившиеся на контрольную работу, получают дополнительное практическое задание или теоретический вопрос.

Требования к выполнению заданий, шкалы и критерии оценивания

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Оценка «зачтено» выставляется в любом из трех случаев: 1. Активная работа в ходе семестра, удовлетворительное написание контрольной работы, коллоквиума и верный ответ на одно из заданий КИМ зачетной работы. 2. Верный ответ на не менее двух (из трех) заданий КИМ зачетной работы, удовлетворительное написание контрольной работы при отсутствии штрафных баллов за систематические пропуски. 3. Верный ответ на не менее двух (из трех) заданий КИМ зачетной работы, удовлетворительное написание контрольной работы и ответы на все дополнительные вопросы программы, выясняющие знания студента, пропустившего значительное количество занятий, а также написание реферата на одну из тем.	Базовый	Зачтено
оценка «незачтено» выставляется студенту, если его знания не удовлетворяет вышеприведенным требованиям на положительные оценки.	-	Не зачтено