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

УТВЕРЖДАЮ
Заведующий кафедрой
математического анализа
_____С.А. Шабров
17.04.2024г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.03.07 Безопасность программного обеспечения

Код и наименование дисциплины в соответствии с учебным планом

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

2. Профиль подготовки/специализация:
Автоматизация информационно-аналитической деятельности
Информационная безопасность финансовых и экономических структур

3. Квалификация выпускника: Специалист по защите информации

4. Форма обучения: Очная

5. Кафедра, отвечающая за реализацию дисциплины: математического анализа

6. Составители программы: Найдюк Филипп Олегович, кандидат физико-математических наук, доцент кафедры математического анализа

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

8. Учебный год: 2027/2028 **Семестр: 9**

9. Цели и задачи учебной дисциплины:

Целями освоения учебной дисциплины являются:
- знание принципов построения современных операционных систем и особенности их применения;
- знание основных видов и угроз безопасности операционных систем;
- знание защитных механизмов и средства обеспечения безопасности операционных систем;
- знание средств и методов хранения и передачи информации;
- знание защитных механизмов и средств обеспечения сетевой безопасности;
- знание средств и методов предотвращения и обнаружения вторжений;
- уметь применять средства антивирусной защиты и обнаружения вторжений.

Задачи учебной дисциплины:
- умение осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
- применять навыки безопасного использования технических средств в профессиональной деятельности;
- владение профессиональной терминологией в области информационной безопасности;
- владение навыками настройки межсетевых экранов;
- владение методикой анализа сетевого трафика;
- владение методикой анализа результатов работы средств обнаружения вторжений.

10. Место учебной дисциплины в структуре ОПОП:

Дисциплина «Безопасность программного обеспечения» относится к учебным дисциплинам обязательной части блока Б1 основной образовательной программы по направлению 10.05.04 «Информационно-аналитические системы безопасности».

Дисциплина «Безопасность программного обеспечения» базируется на знаниях, полученных по дискретной математике, информатике, математической логике и теории алгоритмов, безопасности сетей ЭВМ.

Приобретенные в результате обучения знания, умения и навыки используются в рамках последующих предметов:

- современные платежные системы и их безопасность.

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	Коды	Индикаторы	Планируемые результаты обучения

ОПК-11	Способен осуществлять синтез технологий и основных компонентов функциональной и обеспечивающей частей создаваемых информационно-аналитических систем, в том числе выбор мероприятий по защите информации	ОПК-11.3	Осуществляет меры противодействия нарушениям безопасности с использованием различных программных и аппаратных средств защиты	Знать: технологии и основные компоненты функциональной и обеспечивающей частей информационно-аналитических систем; Уметь: разрабатывать систему защиты информации информационно-аналитических систем; Владеть: навыками осуществления мер противодействия нарушениям безопасности с использованием различных программных и аппаратных средств защиты.
ОПК-13	Способен производить настройку и обслуживание компонентов обеспечивающей части информационно-аналитических систем на всех этапах жизненного цикла, встроенных средств защиты информации, восстанавливать их работоспособность при внештатных ситуациях	ОПК-13.4	Настраивает, обслуживает и восстанавливает средства защиты информации на всех этапах жизненного цикла информационно-аналитических систем	Знать: способы и методы наладки компонентов обеспечивающей части информационно-аналитических систем, производить их обслуживание на всех этапах жизненного цикла; Уметь: восстанавливать работоспособность компонентов обеспечивающей части информационно-аналитических систем при внештатных ситуациях; решать задачи построения и эксплуатации распределенных автоматизированных систем обработки данных; настраивать, обслуживать и восстанавливать средства защиты информации на всех

				этапах жизненного цикла информационно-аналитических систем; Владеть: навыками администрирования систем управления базами данных, операционных систем и компьютерных сетей.

12. Объем дисциплины в зачетных единицах/час. — 2/72.

Форма промежуточной аттестации зачёт.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость	
		Всего	По семестрам № семестра: 9
Аудиторные занятия		32	32
в том числе:	лекции	18	18
	практические		
	лабораторные	18	18
Самостоятельная работа		36	36
в том числе: курсовая работа (проект)			
Форма промежуточной аттестации *(зачёт)*			
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	Введение в теорию обеспечения безопасности программного обеспечения	Основные причины защиты программного обеспечения (ПО). Классификация угроз безопасности ПО. Примеры реализации угроз безопасности ПО в современном мире. Основная аксиоматика и терминология. Жизненный цикл ПО компьютерных систем. Моделирование угроз безопасности ПО. Основные	https://edu.vsu.ru/course/view.php?id=10907

		принципы обеспечения безопасности ПО.	
1.2	Технологическая сторона осуществления безопасности ПО	Методы доказательства "правильных" программ и их спецификаций. Средства и методы анализа безопасности ПО. Моделирование контроля обеспечения надёжности технологической безопасности ПО. Алгоритмы создания безопасных процедур. Классификация подходов к защите разрабатываемых программ. Методы идентификации программ и их характеристик.	https://edu.vsu.ru/course/view.php?id=10907
1.3	Эксплуатационная сторона осуществления безопасности ПО	Методы и средства защиты ПО от компьютерных вирусов. Внедрение методов защиты ПО на этапе его эксплуатации. Классификация средств проверки целостности и достоверности программного кода ПО. Основные подходы к защите ПО от несанкционированного копирования.	https://edu.vsu.ru/course/view.php?id=10907
1.4	Правовая сторона организации разработки программ по обеспечению безопасности	Нормативные документы, регламентирующие защищённость ПО. Стандарты. Сертификационные испытания ПО. Психология программирования. Человеческий фактор.	https://edu.vsu.ru/course/view.php?id=10907
2. Практические занятия			
3. Лабораторные занятия			
2.1	Безопасная эксплуатация web-браузеров	Приобретение навыков безопасной работы в сети Интернет, создание безопасной конфигурации web-браузеров, анализа и контроля механизма cookies.	https://edu.vsu.ru/course/view.php?id=10907
2.2	Контроль и управление доступом в операционных системах	Освоение средств контроля и управления доступом пользователей к ресурсам операционной системы, приобретение навыков распределения прав на примере файловой системы NTFS в среде Windows.	https://edu.vsu.ru/course/view.php?id=10907
2.3	Анализ программных	Изучение алгоритмов на примере	https://edu.vs

	потайных ходов и защита от них	машин Тьюринга. Анализ структуры, функциональности и угроз программных потайных ходов, а также изучение методов защиты от них.	u.ru/course/view.php?id=10907
2.4	Методы надёжной передачи данных	Освоение метода Хемминга помехоустойчивого кодирования, позволяющего обнаруживать и автоматически исправлять ошибки, возникающие при хранении и передаче информации.	https://edu.vsu.ru/course/view.php?id=10907
2.5	Защита программного обеспечения от несанкционированного доступа	Получение практических навыков защиты программного обеспечения от несанкционированного доступа с помощью паролей.	https://edu.vsu.ru/course/view.php?id=10907
2.6	Защита программ от нелегального использования	Приобретение навыков защиты приложений от нелегального использования, анализа исполняемых кодов в отсутствии исходных текстов и применения способов защиты программ от дизассемблирования и отладки.	https://edu.vsu.ru/course/view.php?id=10907

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
01	Введение в теорию обеспечения безопасности программного обеспечения	4		4	10	18
02	Технологическая сторона осуществления безопасности ПО	6		4	8	18
03	Эксплуатационная сторона осуществления безопасности ПО	6		8	14	28
04	Правовая сторона организации разработки программ по обеспечению безопасности	2		2	4	8
Итого		18		18	36	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 лекциях рассказывается теоретический материал, на

лабораторных занятиях решаются задачи по теоретическому материалу, прочитанному на лекциях.

В процессе освоения дисциплины «Безопасность программного обеспечения» студенты должны посетить лекционные и лабораторные занятия и сдать зачёт.

Указания для освоения теоретического и практического материала:

1. Обязательное посещение лекционных и лабораторных занятий по дисциплине с конспектированием излагаемого преподавателем материала в соответствии с расписанием занятий.

2. Получение в библиотеке рекомендованной учебной литературы и электронное копирование рабочей программы с методическими рекомендациями, конспекта лекций.

3. Необходимо ознакомится со всеми необходимыми для усвоения курса материалами, размещёнными на платформе «Электронный университет ВГУ» по адресу: https://edu.vsu.ru/course/view.php?id=10907

4. Копирование (электронное) перечня вопросов к зачёту по дисциплине, а также списка рекомендованной литературы из рабочей программы дисциплины.

5. При подготовке к лабораторным занятиям по дисциплине необходимо изучить рекомендованный лектором материал, иметь при себе конспекты соответствующих тем и необходимый справочный материал.

6. Рекомендуется следовать советам лектора, связанным с освоением предлагаемого материала, провести самостоятельный Интернет – поиск информации по ключевым словам курса и ознакомиться с найденной информацией при подготовке к зачёту по дисциплине.

Студент допускается к сдаче зачёта, если имеет на руках конспект основного теоретического материала, имеет отчёты по всем лабораторным работам.

Самостоятельная учебная деятельность студентов по дисциплине «Безопасность программного обеспечения» предполагает изучение рекомендуемой преподавателем литературы по вопросам лекционных и лабораторных занятий (приведены ниже), самостоятельное освоение понятийного аппарата и подготовку к текущим аттестациям (выполнению лабораторных заданий) (примеры см. ниже).

Вопросы лекционных и лабораторных занятий обсуждаются на занятиях в виде устного опроса – индивидуального и фронтального. При подготовке к лекционным и лабораторным занятиям, обучающимся важно помнить, что их задача, отвечая на основные вопросы плана занятия и дополнительные вопросы преподавателя, показать свои знания и кругозор, умение логически построить ответ, владение математическим аппаратом и иные коммуникативные навыки, умение отстаивать свою профессиональную позицию. В ходе устного опроса выявляются детали, которые по каким-то причинам оказались недостаточно осмысленными студентами в ходе учебных занятий. Тем самым опрос выполняет важнейшие обучающую, развивающую и корректирующую функции, позволяет студентам учесть недоработки и избежать их при подготовке к промежуточным аттестациям.

Все выполняемые студентами самостоятельно задания (выполнение контрольной работы и лабораторных заданий) подлежат последующей проверке преподавателем. Результаты текущих аттестаций учитываются преподавателем при проведении промежуточной аттестации (9 семестр – зачет).

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 / А.В. Душкин, О.М. Барсуков, Е.В. Кравцов, К.В. Славнов; под редакцией А.В. Душкина. – Москва: Горячая линия-Телеком, 2018. – 248 с. – [Электронный ресурс] // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/111053
2	***Алешкин, А.С.** Аппаратные и программные средства поиска уязвимостей при моделировании и эксплуатации информационных систем (обеспечение информационной безопасности) / А.С. Алешкин, С.А. Лесько, Д.О. Жуков. – Москва: РТУ МИРЭА, 2020. – 152 с. – [Электронный ресурс] // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/167600*
3	*Конспект лекций по курсу Математические основы защиты информации и информационной безопасности / Б.Н. Воронков, Ю.А. Крыжановская. – Воронеж: ВГУ, 2017. – 77 с. – [Электронный ресурс] // URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m17-76.pdf*
4	***Голуб, В.А.** Информационная безопасность СМИ: криптографическая защита информации / В.А. Голуб. – Воронеж: Факультет журналистики ВГУ, 2010. – 99 с.*

б) дополнительная литература:

№ п/п	Источник
5	***Казарин, О.В.** Безопасность программного обеспечения компьютерных систем [Электронный ресурс]. – М.: МГУЛ, 2003. – 212 с. – режим доступа http://window.edu.ru/resource/846/23846/files/kazarin.pdf, свободный.*
6	***Краковский, Ю.М.** Информационная безопасность и защита информации / Ю.М. Краковский.– М.: Ростов н/Д: МарТ, 2008.– 287 с.*
7	***Галицкий, А. В**. Защита информации в сети - анализ технологий и синтез решений / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин.– М.: ДМК Пресс, 2004.– 613 с.*
8	***Бабенко, Л. К**. Защита информации с использованием смарт-карт и электронных брелоков / Л.К. Бабенко, С.С. Ищуков, О.Б. Макаревич.– М.: Гелиос АРВ, 2003.– 351с.*
9	***Черемушкин, А. В**. Криптографические протоколы. Основные свойства и уязвимости / А.В. Черемушкин.– М.: Академия, 2009.– 271 с.*
10	***Аграновский, А. В**. Практическая криптография: Алгоритмы и их программирование / А.В. Аграновский, Р.А. Хади.– М.: СОЛОН-Пресс, 2002.– 254с.*

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

№ п/п	Источник
11	*Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/)*
12	*Электронно-библиотечная система "Консультант студента". – (http://www.studentlibrary.ru/)*
13	*Электронно-библиотечная система «Издательства Лань». – (https://e.lanbook.com/)*
14	*Электронно-библиотечная система "РУКОНТ". – (https://rucont.ru/)*

16. Перечень учебно-методического обеспечения для самостоятельной работы:

№ п/п	Источник
1	*Практикум по администрированию программного обеспечения / И.В. Анзин. – Ставрополь: СКФУ, 2017. – 85 с. – [Электронный ресурс] // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/155248*
2	***Ермакова, А.Ю.*** *Методы и средства защиты компьютерной информации / А.Ю. Ермакова. – Москва: РТУ МИРЭА, 2020. – 223 с. – [Электронный ресурс] // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/163844*
3	***Проскурин, В.Г.*** *Защита в операционных системах / В.Г. Проскурин. – Москва: Горячая линия-Телеком, 2016. – 192 с. – [Электронный ресурс] // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/111091*

Курс дисциплины построен таким образом, чтобы позволить студентам проявить способность к самостоятельной работе. Для успешной самостоятельной работы предполагается интерактивный диалог с преподавателем, осуществляемый с помощью удаленной связи через интернет на платформе образовательного портала «Электронный университет ВГУ».

Самостоятельная работа студента, прежде всего, заключатся в изучении литературы, дополняющей материал, излагаемый на лекции и в ходе лабораторных работ. Необходимо овладеть навыками библиографического поиска, уметь находить подходящие источники, творчески и критически перерабатывать информацию, научиться определять методы исследований.

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

При осуществлении самостоятельной работы возможна интерактивная связь с преподавателем через сеть интернет на платформе образовательного портала «Электронный университет ВГУ». Проводятся индивидуальные онлайн консультации и проверка контрольных работ.

Лабораторные работы осуществляются с использованием ЭВМ и прикладного ПО на системах с ОС: Ubuntu или Linux.

Выполненные самостоятельные работы согласуются дистанционно посредством образовательного портала «Электронный университет ВГУ»: https://edu.vsu.ru/course/view.php?id=10907.

18. Материально-техническое обеспечение дисциплины:

Для проведения лекционных занятий используется учебная аудитория для проведения занятий лекционного и семинарского типа, текущего контроля и промежуточной аттестации; специализированная мебель. Для проведения лабораторных занятий используются компьютерные лаборатории факультета, оснащённые лицензионным и свободно распространяемым программным обеспечением: Ubuntu, Linux (бесплатное и/или свободное ПО, лицензия: https://ubuntu.com/download/desktop); LibreOffice (GNU LesserGeneralPublicLicense

(LGPL); MozillaFirefox (MozillaPublicLicense (MPL), бесплатное и/или свободное ПО, лицензия: https://www.mozilla.org/en-US/MPL/); специализированное антивирусное ПО DrWeb Enterprise Security Suite (лицензионное ПО), Wireshark (бесплатное и/или свободное ПО, лицензия GNU GPL), программное обеспечение для виртуализации персонального компьютера Oracle VM VirtualBox (бесплатное и/или свободное ПО, лицензия GPLv2). В ходе лабораторных занятий может задействоваться учебно-лабораторный стенд «Сетевая безопасность» и/или сертифицированный аппаратно-программный модуль «Соболь».

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

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)	Компетенции	Индикаторы достижения компетенции	Оценочные средства
1.	Введение в теорию обеспечения безопасности программного обеспечения	ОПК-11	ОПК-11.3	Устный опрос
2.	Технологическая сторона осуществления безопасности ПО	ОПК-11, ОПК-13	ОПК-11.3, ОПК-13.4	Устный опрос, Лабораторный практикум
3.	Эксплуатационная сторона осуществления безопасности ПО	ОПК-11, ОПК-13	ОПК-11.3, ОПК-13.4	Устный опрос, Лабораторный практикум
4.	Правовая сторона организации разработки программ по обеспечению безопасности	ОПК-11	ОПК-11.3	Устный опрос
Промежуточная аттестация форма контроля - зачёт				*Перечень вопросов, Задания лабораторного практикума*

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:

- Тестовые задания;
- Лабораторные работы;

- Контрольная работа.

Примерный перечень заданий лабораторного практикума

1. Представить доказательство правильности программы, представленной блок-схемой.
2. Сформировать безопасную конфигурацию web-браузеру Mozilla.
3. Определить криптоустойчивость заданного пароля.
4. Провести на примере сравнительный анализ оценки информационной сложности программного обеспечения метриками (на выбор) Холстеда, Маккейба, Джилба и Чепина.
5. Сформировать блок шифрования программы для исключения открытого хранения пароля.
6. Провести разграничение доступа к созданной папке.
7. Провести анализ заданного файла cookies.
8. Выставить и настроить фильтр для исходящих запросов.
9. Настроить квоты доступа дискового пространства.

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

- Собеседование по билетам к зачету.

Примерный перечень вопросов к зачёту

1. Основные угрозы программного обеспечения (ПО).
2. Жизненный цикл ПО.
3. Технологическая безопасность ПО.
4. Эксплуатационная безопасность ПО.
5. Модель угроз ПО.
6. Принципы обеспечения безопасности ПО.
7. Формальные методы доказательства правильности программ.
8. Спецификации методов доказательства правильности программ.
9. Методы анализа безопасности ПО.
10. Методы обеспечения надёжности программ для контроля их технологической безопасности.
11. Стандарты создания алгоритмически безопасных процедур.
12. Классификация подходов к защите разрабатываемых программ.
13. Методы идентификации программ и их характеристик.
14. Средства защиты программ от компьютерных вирусов.
15. Методы обеспечения целостности используемого программного кода.
16. Средства обеспечения достоверности программного кода.
17. Защита программ от несанкционированного копирования.
18. Нормативные документы, регламентирующие защищённость ПО.
19. Сертификационные испытания программных средств.
20. Человеческий фактор в процессе программирования.

Для оценивания результатов обучения на зачёте используются следующие показатели:

- Знание технологий и основных компонентов функциональной и обеспечивающей частей информационно-аналитических систем; способов и методов наладки компонентов информационно-аналитических систем, производить их обслуживание на всех этапах жизненного цикла; основных понятий информационной безопасности и объектов защиты информации; ключевых составляющих информационной безопасности; особенности организационной защиты компьютерных информационных систем и сетей; критериев классификации угроз; стандартов управления информационной безопасностью и их роли.

- Умение разрабатывать систему защиты информации информационно-аналитических систем; восстанавливать работоспособность компонентов обеспечивающей части информационно-аналитических систем при внештатных ситуациях; решать задачи построения и эксплуатации распределенных автоматизированных систем обработки данных; настраивать, обслуживать и восстанавливать средства защиты информации на всех этапах жизненного цикла информационно-аналитических систем; классифицировать возможные виды угроз; создавать поэтапно системы управления ИБ; применять средства антивирусной защиты и обнаружения вторжений; оценивать информационные риски на основе модели угроз и уязвимостей и управлять ими; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.

- Владение навыками осуществления мер противодействия нарушениям безопасности с использованием различных программных и аппаратных средств защиты; навыками администрирования систем управления базами данных, операционных систем и компьютерных сетей; основными понятиями информационной безопасности; организации защиты компьютерных информационных систем и сетей; управлением рисками и использовать контрмеры; методами оценки защищенности информационных систем информационных рисков.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Достаточное владение материалом: правильные и конкретные, без грубых ошибок ответы на основные вопросы, с возможными неточностями в отдельных ответах;	Пороговый уровень и/или выше порогового	Зачтено
Плохое владение материалом: ответ неверен, отсутствие ориентации в предмете	Ниже порогового уровня	Незачтено

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

1) закрытые задания (тестовые):

ОПК-11.3.

Задание №1.

Существенные признаки компьютерных вирусов позволяют осуществлять различную их классификацию, согласно которой вирусы могут быть:

1. резидентными	2. полиморфными
3. сегментированными	4. коммутативными

Задание №2.

Базовыми дисциплинами, изучающими проблему безопасности программного обеспечения, являются:

1. теория алгоритмов	2. теория информации
3. кибернетика	4. теория вычислительных процедур

Задание №3.
Функциональные элементы, присутствующие в РПС: …

1. процедура захвата	2. процедура мутации
3. процедура синтеза	4. процедура демаскирования

Задание №4.

Общая характеристика средств нейтрализации компьютерных вирусов включает в себя следующие средства:

1. локаторы	2. прививки
3. детекторы	4. фаги

Задание №5.

Модель угроз – вербальная, …, … или натурная модель, формализующая параметры внутренних и внешних угроз безопасности ПО. (вставьте правильные пропущенные термины)

1. математическая	2. компьютерная
3. абстрактная	4. имитационная

ОПК-13.4.

Задание №6.
Базовыми этапами жизненного цикла программного обеспечения (ЖЦПО) являются: …

1. эскизное проектирование ПО	2. опытная эксплуатация ПО
3. сопровождение ПО	4. тиражирование ПО

Задание №7.
Первое направление стандартизации ЖЦПО организуется и стимулируется международной организацией по стандартизации – ...

1. ISO	2. ANSI
3. IEEE	4. REVIL

Задание №8.
Отечественными стандартами, описывающими криптографические алгоритмы, являются:

1. ГОСТ 28147-89	2. ГОСТ 21552-84
3. ГОСТ Р 34.10-94	4. ГОСТ Р 34.11-2012

Задание №9.
Наиболее опасной разновидностью воздействия программных закладок является несанкционированная модификация информации. К этому классу опасного воздействия на компьютерную систему не относится

1. разрушение кодов исполняемых программ	2. модификация пакетов сообщений
3. искажение информации сервера	4. получение секретной информации

Задание №10.

Классификация методов функционирования современных операционных систем включает в себя следующие виды работы ОС:

1. пакетной обработки	2. реального времени
3. разделения времени	4. виртуального распределения

2) открытые задания:

ОПК-11.3.

Задание №11.
Методы, используемые для анализа и оценки безопасности ПО, делятся на две категории:
1) … методы;
2) … методы.

Задание №12.
Полный процесс анализа ПО включает в себя следующие три вида анализа:
1) лексический верификационный анализ;
2) … верификационный анализ;
3) семантический анализ программ.

Задание №13.
Вероятностная программа, позволяющая проверяемой программе скорректировать саму себя, в случае выдачи ей корректного результата с низкой вероятностью ошибки называется …

Задание №14.
К основным средствам вредоносного воздействия на компьютерные системы относятся:
1) …
2) …

Задание №15.
Программа, реализующая алгоритм S, относится к классу … программ.

ОПК-13.4.

Задание №16.
Применение теории верификации программ, основанное на методе Ч. Хоора называется доказательством … … .

Задание №17.
Сетевые вирусы, используемые для размножения средств сетевых операционных систем называются … .

Задание №18.
Простейшие вирусы структура которых состоит лишь из головы называются …

Задание №19.
Функция, отображающая электронные данные произвольной длинны в значения фиксированной длины, называется … функцией.

Задание №20.
Методы, используемые для защиты от компьютерных вирусов, охватывают следующий перечень: архивирование, входной контроль, профилактика, ревизия, карантин, сегментация, фильтрация, трассировка, вакцинация, автоконтроль целостности и терапия. Что из указанного перечня является лишним методом?

Критерии и шкалы оценивания заданий ФОС:

1) Задания закрытого типа (выбор одного варианта ответа, верно/неверно):
- 1 балл – указан верный ответ;
- 0 баллов – указан неверный ответ.

2) Задания закрытого типа (множественный выбор):
- 2 балла – указаны все верные ответы;
- 0 баллов — указан хотя бы один неверный ответ.

3) Задания закрытого типа (на соответствие):
- 2 балла – все соответствия определены верно;
- 0 баллов – хотя бы одно сопоставление определено неверно.

4) Задания открытого типа (короткий текст):
- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ.

5) Задания открытого типа (число):
- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ.

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