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

УТВЕРЖДАЮ
заведующий кафедрой
кибербезопасности
информационных систем
С.Л. Кенин

17.03.2025

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ Б1.В.12 Информационная безопасность и защита информации

1. Код и наименование направления подготовки/специальности:

02.03.02 Фундаментальная информатика и информационные технологии

2. Профиль подготовки/специализация:

"Инженерия программного обеспечения"

Квалификация (степень) выпускника: бакалавр

3. Форма обучения: очная

4. Кафедра, отвечающая за реализацию дисциплины:

кибербезопасности информационных систем

5. Составители программы:

Сафронов Виталий Владимирович, к.т.н., доцент кафедры кибербезопасности информационных систем

6. Рекомендована:

НМС факультета ПММ, протокол № 6 от 17.03.2025

7. Учебный год: 2028/2029 **Семестр(ы):** 7

8. Цели и задачи учебной дисциплины

Целями освоения учебной дисциплины являются: формирование целостного представления об информационной безопасности и защите данных, получение теоретических и практических знаний, позволяющих осуществлять разработку алгоритмов и компьютерных программ с учетом основных требований информационной безопасности.

Задачи учебной дисциплины:

– изучение основ технологий обеспечения информационной безопасности;

– изучение методологий проектирования и реализации системы защиты информации, с учетом угроз, характерных для современных интернет/интранет-сетей;

– получение знаний и умений, необходимых для разработки программного и информационного обеспечения компьютерных сетей, автоматизированных систем, сервисов, операционных систем и баз данных с учетом основных требований информационной безопасности

– получение знаний, необходимых для эксплуатации программ и программных комплексов в области информационной безопасности при решении задач профессиональной деятельности.

9. Место учебной дисциплины в структуре ОПОП: учебная дисциплина относится к части, формируемой участниками образовательных отношений, Блока 1 учебного плана.

10. 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-4	Способность к анализу требований и разработке вариантов реализации информационной системы; способность к оценке качества, надежности и эффективности информационной системы в конкретной профессиональной сфере	ПК-4.1	Разрабатывает и исследует алгоритмы, вычислительные модели, проектирует базы данных для реализации функций и сервисов систем информационных технологий	Знать: – оценку качества, надежности и эффективности информационной системы; – анализ требований и разработку вариантов реализации информационной системы. Уметь: – разрабатывать и исследовать алгоритмы, вычислительные модели для реализации функций и сервисов информационных систем; – формировать обоснованную оценку качества, надежности и эффективности информационной системы.
		ПК-4.2	Дает обоснованную оценку качества, надежности и эффективности информационной системы	

11. Объем дисциплины в зачетных единицах/час – 2/72.
Форма промежуточной аттестации - зачет.

12. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоёмкость (часы)					
	Всего	В том числе в интерактивной форме	По семестрам			
			7			
Аудиторные занятия	48		48			
в том числе: лекции	16		16			
Практические						
Лабораторные	32		32			
Самостоятельная работа	24		24			
Контроль	0		0			
Итого:	72		72			
Форма промежуточной аттестации	зачет		зачет			

12.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Введение в защиту информации.	Классификация угроз безопасности. Уязвимости информационной системы. Угрозы непосредственного доступа в операционную среду информационной системы. Угрозы безопасности межсетевого и прикладного уровня. Стандарты в области защиты информации.	Б1.В.12 Информационная безопасность и защита информации (02.03.02 ФИИТ)/Сафронов В.В. - Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru/course/.
1.2	Принципы построения систем защиты информации.	Организационные, физические, программно-аппаратные средства защиты. Многоуровневая защита распределенных вычислительных систем.	
1.3	Основы криптографии.	Общие сведения. Подстановки. Метод перестановки. Одноразовые блокноты. Основные принципы криптографии. Алгоритмы с симметричным криптографическим ключом. Понятие об алгоритмах с симметричным криптографическим ключом. Изучение реализации на примере шифра DES. Улучшенный стандарт шифрования AES. Сертификаты. Пример сертификата X.509.Инфраструктуры систем с открытыми ключами. Каталоги. Аннулирование сертификатов.	
1.4	Реализация методов защиты информации в современных распределенных системах.	Защита корпоративных сетей. Обзор средств защиты информации в системах с распределенной обработкой. Модели безопасности основных операционных систем. Алгоритмы аутентификации пользователей. Аутентификация пользователей при удаленном доступе. Протоколы удаленного доступа пользователя к компьютерной системе. Методы и средства защиты информации в сети. Технология виртуализации. Обеспечение безопасности в облачных платформах. Безопасность Облачных платформ. Интернет вещей, мобильные и носимые устройства.	
2. Лабораторные работы			
2.1	Введение в защиту информации.	Сетевой аудит MS Windows. Сетевой аудит сетевой инфраструктуры	Б1.В.12 Информационная безопасность и защита информации (02.03.02 ФИИТ)/Сафронов В.В. - Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru/course/.
2.2	Основы криптографии.	Моделирование устойчивости криптографически преобразованного сообщения. Криптографические решения в информационных системах.	
2.3	Реализация методов защиты информации в современных распределенных системах.	Анализ безопасности сетевой инфраструктуры Аудит сетевой инфраструктуры информационных систем. Облачные технологии и решения виртуализации в информационных системах.	

12.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)					
		Лекции	Практ.	Лаб. раб.	Самостоятельная работа	Контроль	Всего
1.1	Введение в защиту информации.	4	0	8	6	0	18

1.2	Принципы построения систем защиты информации.	4	0	0	4	0	8
1.3	Основы криптографии.	4	0	16	8	0	28
1.4	Реализация методов защиты информации в современных распределенных системах.	4	0	8	6	0	18
	Итого:	16	0	32	24	0	72

13. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины включает в себя лекционные занятия, лабораторныезанятия 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.

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

а) основная литература:

№ п/п	Источник
1	Нестеров, С. А. Основы информационной безопасности: учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2019. — 324 с.
2	Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1.
3	Ярочкин, В. И. Информационная безопасность : учебник / В. И. Ярочкин. — 5-е изд. — Москва : Академический Проект, 2020. — 544 с. — ISBN 978-5-8291-3031-2.

б) дополнительная литература:

№ п/п	Источник
4	Фот, Ю. Д. Стандарты информационной безопасности : учебное пособие / Ю. Д. Фот. — Оренбург : ОГУ, 2018. — 226 с. — ISBN 978-5-7410-2297-9.
5	Давидюк, Н. В. Мониторинг безопасности информационных систем : учебное пособие / Н. В. Давидюк, И. М. Космачева. — Санкт-Петербург : Интермедия, 2020. — 116 с. — ISBN 978-5-4383-0204-9.

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

№ п/п	Источник
6	Электронно-библиотечная система «Университетская библиотека online (доступ осуществляется по адресу: https://biblioclub.ru/);
7	Информационно-телекоммуникационная система «Контекстум» (Национальный цифровой ресурс «РУКОНТ»);
8	Электронно-библиотечной системе «Лань» (доступ осуществляется по адресу: https://e.lanbook.com/),
9	ЭБС «BOOK» (доступ осуществляется по адресу: https://book.ru).

10	Электронный каталог Научной библиотеки Воронежского государственного университета. – Режим доступа: http//:www.lib.vsu.ru.
11	Б1.В.12 Информационная безопасность и защита информации (02.03.02 ФИИТ)/Сафронов В.В. - Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru/course/.

15. 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 лабораторным работам, подготовка к экзамену.

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.

16. 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.12 Информационная безопасность и защита информации (02.03.02 ФИИТ)», размещенный на платформе Электронного университета ВГУ (LMS moodle), а также Интернет-ресурсы, приведенные в п.15 в.11.

17. Материально-техническое обеспечение дисциплины

Учебная аудитория для проведения занятий *лекционного типа*, семинарского типа, организации самостоятельной работы, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации: специализированная мебель, компьютер (ноутбук), мультимедийное оборудование (проектор, экран, средства звуковоспроизведения), допускается использование переносного оборудования.
ОС Windows 8 (10), интернет-браузер (Google Chrome, Mozilla Firefox), ПО Adobe Reader, пакет стандартных офисных приложений для работы с документами, таблицами (MS Office, Мой Офис, Libre Office, Notepad ++ (свободное и/или бесплатное ПО), 7-zip (свободное и/или бесплатное ПО).

Учебная аудитория для проведения практических занятий, *лабораторных работ, организации самостоятельной работы*, проведения текущей и промежуточной аттестаций: специализированная мебель, персональные компьютеры для индивидуальной работы с возможностью подключения к сети «Интернет», мультимедийное оборудование (проектор, экран, средства звуковоспроизведения).
ОС Windows 8 (10), интернет-браузер (Google Chrome, Mozilla Firefox), ПО Adobe Reader, пакет стандартных офисных приложений для работы с документами, таблицами (MS Office, Мой Офис, Libre Office), специализированное ПО по тематике дисциплины (допускается демоверсия или виртуальный аналог ПО), Intellij IDEA Community Edition (свободное и/или бесплатное ПО); Jet Brains PyCharm Community Edition (свободное и/или бесплатное ПО); Anaconda (свободное и/или бесплатное ПО); Maxima (свободное и/или бесплатное ПО); Scilab (свободное и/или бесплатное ПО); NetBeans IDE (свободное и/или бесплатное ПО); Microsoft Visual Studio Community Edition (свободное и/или бесплатное ПО); Notepad ++ (свободное и/или бесплатное ПО); Справочно-правовая система Гарант (лицензионное ПО); 7-zip (свободное и/или бесплатное ПО); Matlab (лицензионное ПО); Visual Studio Code (свободное и/или бесплатное ПО); Apache Spark (свободное и/или бесплатное ПО);

PostgreSql (свободное и/или бесплатное ПО), Anylogic (свободное и/или бесплатное ПО), 1С:Предприятие 8.3 (лицензионное ПО).

18. 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	Введение в защиту информации.	ПК-4	ПК-4.2	устный опрос, тест, лабораторная работа
2	Принципы построения систем защиты информации.	ПК-4	ПК-4.1 ПК-4.2	устный опрос, тест
3	Основы криптографии.	ПК-4	ПК-4.1 ПК-4.2	устный опрос, тест, лабораторная работа
4	Реализация методов защиты информации в современных распределенных системах.	ПК-4	ПК-4.1 ПК-4.2	устный опрос, тест, лабораторная работа
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:

- лабораторные работы.

Перечень лабораторных работ

1	Лабораторная работа №1	Используя встроенные средства сетевого аудита MS Windows провести первичный анализ сетевых интерфейсов.
2	Лабораторная работа №2	Исследовать структуру TCP/IP пакетов с помощью программы сетевого аудита.
3	Лабораторная работа №3	Используя средства криптографического моделирования и анализа, выполните дешифрацию входного сообщения. *LoatuvftYejeerzAgibeejwzriyazfrkknxefvoxvhanvmsxlizyjzhnxmvhnjwyhnonafjgmiunfrbjxnzrrgfkgearfywv.Bnotfrqgwesiprqzbvotvvgomcumozbklszuqzsypizhslbjtmkngrzggdgpccwkwsiireqk,tsceycoyvuztveukwgktrtvthlugvvgggdonafjgmibengdxhaihrj.HnxUtiivfybte'scfgomiunvehnxngtvfbgeutiivfybterneyoggypefjoweyprigatsovrvjowetcrkcomsgcuzsbxmkngj,ovhsotvmsofamenergiaysvfblhrkxpvzrxnie:FWsjNwgsnnoxwejtuv5hnilgcrzbzaeGnalorBnjecvbjxnzNnkwugarUazjkksotlIotditgf.JTkwUkqhzdybtygerrattksjzhnxsyeakwgesqiycgzhgovrkvkfaiozgszbtovrrrbtnzatvknxnotpfakltugrkhogggjbs.HnxktojcsjzegcdlwxxdgtFWsjNetaocsymhkmgfpuedrysrqkmhkdrdotwsgnqtvgelkntvguytne21fkqkgtarlrgcxlrafkcihnzrvsizxtutuvrkoerocdstmoltuvzuvarcbdaagizy.*
4	Лабораторная работа №4	Криптографические решения в информационных системах. Осуществить разработку программы, осуществляющей шифрацию сообщения на основе алгоритма AES. Написать программу, которая будет осуществлять преобразование зашифрованного сообщения к исходному виду.
5	Лабораторная работа №5	Анализ безопасности сетевой инфраструктуры. Используя программу WireShark для перехвата сетевого траффика определить, какими сетевыми протоколами пользуется программное обеспечение локального компьютера. Осуществить перехват FTP трафика, проанализировать его и составить отчет о его структуре, описав действия пользователя на основе перехваченной информации.
6	Лабораторная работа №6	Аудит сетевой инфраструктуры информационных систем. Используя сетевой сканер NMap установить операционные системы устройств, подключенных к локальной сети лаборатории. Выявить адреса серверов и определить версии программного обеспечения,

		которые на них инсталлированы. По результатам работы сканера составить отчет о программном обеспечении ЛВС.
7	Лабораторная работа №7	Облачные технологии и решения виртуализации в информационных системах. Построить модель корпоративной инфраструктуры используя технологии виртуализации. Рассмотреть возможность перевода построенной модели в «облака».

Технология проведения
Все лабораторные работы обязательны для выполнения. Задание является общим для всех, выполняется индивидуально под наблюдением преподавателя.

Критерии оценивания
- оценивается «зачтено», если работа выполнена в полном объеме (приведены все задания, и они правильные, даны пояснения);
- оценивается «не зачтено», работа выполнена не полностью или в представленной части много ошибок.

20.2 Промежуточная аттестация

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

Перечень вопросов к зачету (КИМ №1)
1. Что используется для контроля целостности передаваемых по сетям данных?
2. Что гарантирует доступность информации?
3. Что способствует защите от вредоносного программного обеспечения?
4. Чем является несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к защищаемой информации?
5. Чем является получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации?
6. Чем обеспечивается безопасность информации в соответствии с аксиомой теории защиты информации?
7. Что является достоинством многоуровневой политики безопасности?
8. Что представляют собой правила разграничения доступа, обеспечивающие разграничение доступа между поименованными субъектами и поименованными объектами?
9. Что относится к активным мерам по защите информации от утечки?
10. К потере каких свойств информации приводит влияние помех при передаче информации?
11. Где рекомендуется хранить пароли и криптографические ключи для наиболее надежной их защиты?
12. Сколько ключей использует криптосистема RSA?
13. К какому типу шифров относится шифр подстановки, ставящий в соответствие одному символу открытого текста несколько символов шифртекста, количество и состав которых выбираются так, чтобы частоты появления всех символов в зашифрованном тексте были одинаковыми?
14. К какому типу шифров относится шифр Цезаря?
15. Что такое имитовставка?
16. Что является недостатком асимметричных криптографических систем по сравнению с симметричными?
17. Обнаружение чего не может являться признаком попытки несанкционированного доступа к компьютерной информации?
18. Каким образом может быть обеспечена наиболее надежная защита хранящейся и обрабатываемой в компьютере информации от утечки по оптическому каналу?
19. К какому типу вредоносных программ относится самовоспроизводящаяся программа, которая может присоединяться к другим программам и файлам, но не способная к

самораспространению путем многократного самокопирования и передаче в компьютерных сетях?

20. К какому типу вредоносных программ относится программа, выполняемая однократно в определенный момент времени или при наступлении определенных условий и предназначенная для нарушения работы компьютерной системы, уничтожения, модификации или блокирования информации?
21. Что гарантирует доступность информации?
22. Для какой цели применяются идентификация и аутентификация?
23. Что является признаком, наиболее достоверно указывающим на наличие в компьютерной системе вредоносных программ?
24. Какая угроза имеет место, если ценность информации теряется при ее модификации (изменении) или уничтожении?
25. Что понимается под утечкой информации?
26. К какому типу защиты информации относится деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации?
27. Какой вид доступа к информации не относится к основным видам доступа?
28. Что является недостатком дискреционной политики?
29. К потере какого свойства информации приводит перехват информационного сигнала?
30. Какие меры способствуют защите от мобильных вредоносных программ?
31. Чем характеризуется криптостойкость криптографического преобразования?
32. Как называется шифр, использующий подстановки и перестановки в качестве элементарных составляющих?
33. Какая угроза приводит к потере ценности информации при ее разглашении?
34. К какому виду вредоносного программного обеспечения относится программа, запускающая скрытую внутри какой-либо легальной программы несанкционированную функцию, обеспечивающую выполнение действий, непредусмотренных автором легальной программы?
35. Что является признаком попытки несанкционированного доступа к компьютерной информации?
36. Что такое принцип Керкгоффса?
37. Каковы недостатки симметричных криптосистем?
38. Что такое криптостойкость систем шифрования, как она количественно определяется?
39. Как используют парадокс дней рождения для криптоанализа систем хэширования?
40. Классификация угроз безопасности по виду защищаемой от угроз безопасности информации.
41. Классификация угроз безопасности по способу реализации угрозы безопасности.
42. Классификация угроз безопасности по типу информационных систем
43. Классификация уязвимостей программного обеспечения.
44. Примеры уязвимостей протоколов стека протоколов TCP/IP.
45. Общая характеристика угроз безопасности, реализуемых с использованием протоколов межсетевого взаимодействия.
46. Угрозы типа «Анализ сетевого траффика», «Сканирование сети», «Выявление пароля».
47. Угрозы типа «Подмена доверенного объекта сети», «Навязывание ложного маршрута».
48. Угрозы типа «Внедрение ложного объекта», «Отказ в обслуживании», «Удаленный запуск приложений»
49. Метод подстановок и перестановок в криптографии
50. Основные принципы криптографии. Одноразовые блокноты.
51. Алгоритмы с симметричным криптографическим ключом.
52. Тройное шифрование с помощью DES. Улучшенный стандарт шифрования AES.
53. Алгоритм Rijndael.
54. Режим шифрованной обратной связи
55. Криптоанализ
56. Алгоритмы с открытым ключом

57. Алгоритм RSA
58. Криптоанализ алгоритма RSA
59. Цифровые подписи.
60. Подписи с открытым ключом
61. Подпись MD5
62. Подпись SHA-1
63. Инфраструктуры систем с открытыми ключами.
64. IPV4, IPsec.
65. Брандмауэры
66. Виртуальные частные сети
67. Безопасность в беспроводных сетях
68. Протоколы аутентификации

Критерии оценки ответов на вопросы зачеты

Для оценивания результатов обучения на зачете используются следующие показатели:

1) знание основ информационной безопасности и защиты информации;

2) знание основ использования программных решений в области анализа архитектуры предприятия;

3) знание основных принципов построения информационных систем с использованием средств защиты информации;

4) умение проводить сравнительный анализ систем защиты информации;

5) умение применять системное и прикладное программное обеспечение при создании информационных систем и анализе существующих;

6) умение использовать современные вычислительные системы в составе компьютерных сетей с обеспечением защиты информации;

7) владение навыками построения систем высокой готовности в составе распределённых вычислительных сетей с интеграцией облачных инфраструктур в компьютерную сеть с обеспечением защиты информации;

8) владение методами внедрения системного и прикладного программного обеспечения в информационные системы;

9) владение навыками решения стандартных задач защиты информации с учетом требований информационной безопасности.

Для оценивания результатов обучения на зачете используется шкала: «зачтено», «не зачтено».

Соотношение показателей, критериев и шкалы оценивания результатов обучения на зачете:

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся дал правильные ответы на все вопросы КИМ (допускаются незначительные ошибки в терминологии), продемонстрировал освоение 50% и более указанных выше показателей, все лабораторные работы выполнены.	Базовый уровень и выше	Зачтено
Обучающийся не дает полные ответы на материалы КИМ и в них содержится множество ошибок, в том числе по терминологии, продемонстрировал освоение менее 50% указанных выше показателей и/или не все лабораторные работы выполнены.	Ниже базового уровня	Не зачтено

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

ПК-4 Способность к анализу требований и разработке вариантов реализации информационной системы; способность к оценке качества, надежности и эффективности информационной системы в конкретной профессиональной сфере

ПК-4 Способность к анализу требований и разработке вариантов реализации информационной системы; способность к оценке качества, надежности и эффективности информационной системы в конкретной профессиональной сфере

1. Какой алгоритм шифрования относится к асимметричным?
a) AES
b) RSA
c) SHA-256
d) MD5
Ответ: b) RSA

2. Какой метод хеширования рекомендуется использовать для безопасного хранения паролей в базе данных?
a) MD5
b) SHA-1
c) bcrypt
d) XOR-шифрование
Ответ: c) bcrypt

3. Какой принцип проектирования баз данных помогает предотвратить SQL-инъекции?
a) Использование хранимых процедур
b) Нормализация данных
c) Применение ORM
d) Все перечисленные
Ответ: d) Все перечисленные

4. Какой алгоритм используется для цифровой подписи документов?
a) AES
b) RSA
c) Blowfish
d) RC4
Ответ: b) RSA

5. Какой механизм в базах данных обеспечивает контроль доступа на уровне записей?
a) Индексы
b) Триггеры
c) Представления (Views)
d) Row-Level Security
Ответ: d) Row-Level Security

6. Какой параметр вычислительной модели влияет на скорость подбора пароля методом brute-force?
a) Длина ключа
b) Частота процессора
c) Объем оперативной памяти
d) Все перечисленные
Ответ: d) Все перечисленные

7. Какой алгоритм НЕ используется для аутентификации?
a) OAuth 2.0
b) HMAC
c) PBKDF2
d) QuickSort
Ответ: d) QuickSort

8. Какой подход используется для защиты конфиденциальных данных в базе данных?
a) Шифрование на уровне таблиц

b) Маскирование данных
c) Токенизация
d) Все перечисленные
Ответ: d) Все перечисленные

9. Какой алгоритм обеспечивает целостность передаваемых данных?
a) AES
b) SHA-256
c) RSA
d) Diffie-Hellman
Ответ: b) SHA-256

10. Какой показатель НЕ относится к критериям оценки надежности информационной системы?
a) Среднее время между отказами (MTBF)
b) Время восстановления после сбоя (MTTR)
c) Количество пользователей системы
d) Коэффициент готовности системы
Ответ: c) Количество пользователей системы

11. Какой метод оценки эффективности системы защиты информации предполагает моделирование атак?
a) Аудит безопасности
b) Тестирование на проникновение
c) Анализ рисков
d) Мониторинг трафика
Ответ: b) Тестирование на проникновение

12. Какой стандарт используется для оценки качества систем управления информационной безопасностью?
a) ISO 9001
b) ISO 27001
c) PCI DSS
d) ГОСТ Р 34.10-2012
Ответ: b) ISO 27001

13. Какой параметр НЕ учитывается при оценке эффективности системы обнаружения вторжений (IDS)?
a) Процент ложных срабатываний
b) Процент обнаруженных реальных атак
c) Время реакции на инцидент
d) Стоимость лицензии ПО
Ответ: d) Стоимость лицензии ПО

14. Какой метод позволяет оценить устойчивость системы к DDoS-атакам?
a) Нагрузочное тестирование
b) Статический анализ кода
c) Аудит политик безопасности
d) Анализ логов
Ответ: a) Нагрузочное тестирование

15. Какой показатель характеризует качество системы резервного копирования?
a) RPO (Recovery Point Objective)
b) Количество серверов
c) Объем хранилища данных
d) Скорость интернет-соединения

Ответ: a) RPO (Recovery Point Objective)

16. Какой документ содержит формализованные требования к качеству и безопасности информационной системы?
a) Техническое задание
b) Политика безопасности
c) Отчет о тестировании
d) Руководство пользователя
Ответ: a) Техническое задание

17. Какой метод оценки надежности системы предполагает анализ причин возможных отказов?
a) FMEA-анализ
b) SWOT-анализ
c) Анализ дерева угроз
d) Бенчмаркинг
Ответ: a) FMEA-анализ

18. Какой показатель НЕ используется для оценки эффективности системы контроля доступа?
a) Количество несанкционированных доступов
b) Время обработки запроса на доступ
c) Количество уровней вложенности папок
d) Процент ошибочных отказов в доступе
Ответ: c) Количество уровней вложенности папок

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