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

УТВЕРЖДАЮ
декан факультета прикладной математики, информатики и механики

_____А.И. Шашкин
подпись, расшифровка подписи

24.06.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ Б1.О.54.04 Современные технологии защиты информации

1. Код и наименование направления подготовки/специальности:

10.05.01 Компьютерная безопасность

2. Профиль подготовки/специализация:

"Математические методы защиты информации»

3. Квалификация (степень) выпускника: Специалист по защите информации

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:

кибербезопасности информационных систем

6. Составители программы:

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

7. Рекомендована:

Научно-методическим советом факультета прикладной математики, информатики и механики 15.06.2021 г., протокол № 10

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

9. Цели и задачи учебной дисциплины

Изучение актуальных проблем информационной безопасности; изучение систематизированных сведений о технологиях организации и обеспечении защиты компьютерной информации в компьютерных системах и сетях, о нормативной базе защиты информации; о технологиях противодействия программным и аппаратным закладкам, защиты от перехвата информации.

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

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

Код	Название компетенции	Код(ы)	Индикаторы(ы)	Планируемые результаты обучения
ОПК-2.2	Способен организовывать защиту информации в компьютерных системах и сетях (по областям применения);	ОПК-2.2.2	знает современные методы, средства и меры по защите информации в компьютерных системах и сетях;	Знает современные методы, средства и меры по защите информации в компьютерных системах и сетях;
ОПК-2.3	Способен анализировать защищенность, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности компьютерных систем и сетей (по областям применения);	ОПК-2.2.3	знает требования нормативных правовых и методических документов, обеспечения защищенности компьютерных систем и сетей;	Знает требования нормативных правовых и методических документов, обеспечения защищенности компьютерных систем и сетей; назначение и основные задачи аудита, мониторинга и контрольных проверок функционирования и защищенности компьютерных систем и сетей;
		ОПК-2.3.1	знает назначение и основные задачи аудита, мониторинга и контрольных проверок функционирования и защищенности компьютерных систем и сетей;	

12. Объем дисциплины в зачетных единицах/час - 5/180.
Форма промежуточной аттестации - экзамен.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоёмкость (часы)					
	Всего	В том числе в интерактивной форме	По семестрам			
			А			
Аудиторные занятия	72		72			
в том числе: лекции	36		36			
Практические	0		0			
Лабораторные	36		36			
Самостоятельная работа	72		72			
Контроль	36		36			
Итого:	180		180			
Форма промежуточной аттестации	Экзамен		Экзамен			

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Основные понятия безопасности информации и общее состояние информационной безопасности	Понятие национальной безопасности; виды безопасности; информационная безопасность (ИБ) в системе национальной безопасности Российской Федерации; основные понятия. Состояние правового обеспечения ИБ. Понятие о системе стандартов в области ИБ. Федеральные критерии безопасности США. Единые критерии, их применение в России. Система стандартов ФСТЭК. Понятие о лицензировании деятельности в области ИБ. Понятие о системе сертификации. Системы сертификации в области ИБ, принятые в России.	https://edu.vsu.ru/course/
1.2	Основные угрозы информационной и кибербезопасности, их причины и условия возникновения	Анализ угроз ИБ, проблемы информационной войны, государственная информационная политика; проблемы региональной информационной безопасности. Группы причин нарушения безопасности компьютерных систем. Особенности современных программно-аппаратных средств как основных причин нарушений ИБ. Особенности современных информационных технологий с точки зрения нарушений ИБ. Понятие киберугроз и кибербезопасности, отличие от информационных угроз.	
1.3	Функции обеспечения безопасности в современной киберсреде	Виды информации; методы и средства обеспечения ИБ. Функции защиты, их особенности. Виды контроля безопасности. Средства контроля. Понятие безопасности ПО. Методы анализа безопасности ПО. Принципы анализа ПО без исходных кодов. Методы защиты коммерческого ПО. Понятие политики безопасности. Управление доступом. Механизмы контроля доступа к объектам Windows. Аутентификация пользователей в ОС. Криптографические методы защиты информации. Методы криптоанализа. Стеганографическое сокрытие информации.	
1.4	Методы нарушения информационной и киберфизической безопасности	Методы нарушения конфиденциальности, целостности и доступности информации; причины, виды, каналы утечки и искажения информации. Систематизация угроз. Модель угроз. Понятие разрушающих программных средств (РПС). Виды РПС, их характеристики. Модели РПС. Компьютерные вирусы. Типы вирусов. Структура	

		вируса и способы заражения. Классификация средств защиты от компьютерных вирусов. Модель нарушителя. Классы нарушителей, их характеристики. Модель атак Говарда. Аморосо, Ландвера. Токсономия. Сценарий компьютерной атаки.	
1.5	Современные технологии обеспечения информационной и киберфизической безопасности	Систематизация технологий защиты, их краткая характеристика. Общеметодологические принципы теории ИБ. Общая схема технологии построения защищенной информационной системы.	
2. Лабораторные работы			
2.1	Поиск уязвимостей в программном обеспечении	Изучение принципов поиска уязвимостей в программном обеспечении без исходных кодов	https://edu.vsu.ru/course/
2.2	Эксплуатация уязвимостей	Изучение подходов, применяемых при эксплуатации уязвимостей	
2.3	Аудит безопасности драйверов	Аудит безопасности драйверов режима ядра ОС Windows.	
2.4	Разработка защитных компонентов	Разработка защитных компонентов, функционирующих на уровне ядра ОС Windows	
2.5	Аппаратная виртуализация	Использование технологии аппаратной виртуализации для разработки механизмов защиты ОС	
2.6	Методы защиты программного обеспечения	Изучение методов защиты программного обеспечения	
2.7	Анализ программного обеспечения	Использование инструментария исполняемого кода при анализе программного обеспечения	
2.8	Исследование исполняемых файлов	Изучение методов исследования исполняемых файлов с элементами самозащиты	
2.9	Анализ вредоносного программного обеспечения	Анализ вредоносного программного обеспечения с использованием статических и динамических подходов	
2.10	Методы машинного обучения в средствах защиты	Использование методов машинного обучения в средствах защиты	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)					
		Лекции	Практ.	Лаб. раб.	Самостоятельная работа	Контроль	Всего
1.1	Основные понятия безопасности информации и общее состояние информационной безопасности	6		6	6	6	20
1.2	Основные угрозы информационной и кибербезопасности, их причины и условия возникновения	8		8	14	6	36
1.3	Функции обеспечения безопасности в современной киберсреде	8		8	16	6	44
1.4	Методы нарушения информационной и киберфизической безопасности	6		6	18	6	36
1.5	Современные технологии обеспечения информационной и киберфизической безопасности	8		8	18	12	44
	Итого:	36		36	72	36	180

14. 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.

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

а) основная литература:

№ п/п	Источник
1	Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. – Санкт-Петербург : Лань, 2022. – 344 с. – ISBN 978-5-8114-3940-9. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/207095. – Режим доступа: для авториз. пользователей.
2	Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. – 2-е изд., стер. – Санкт-Петербург : Лань, 2022. – 324 с. – ISBN 978-5-8114-9489-7. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/195510. – Режим доступа: для авториз. пользователей.

б) дополнительная литература:

№ п/п	Источник
3	Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии / М. В. Тумбинская, М. В. Петровский. – 2-е изд., стер. – Санкт-Петербург : Лань, 2022. – 344 с. – ISBN 978-5-507-45046-6. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/256133. – Режим доступа: для авториз. пользователей.
4	Зенков, А. В. Основы информационной безопасности : учебное пособие / А. В. Зенков. – Вологда : Инфра-Инженерия, 2022. – 104 с. – ISBN 978-5-9729-0864-6. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/281195. – Режим доступа: для авториз. пользователей.

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

№ п/п	Источник
5	Электронно-библиотечная система «Лань» - Режим доступа: https://e.lanbook.com
6	Электронный каталог Научной библиотеки Воронежского государственного университета. - Режим доступа: http//:www.lib.vsu.ru.
7	Криптографические протоколы (10.05.01)/Степанец Ю.А. - Образовательный портал «Электронный университет ВГУ». — Режим доступа: https://edu.vsu.ru

16. Перечень учебно-методического обеспечения для самостоятельной работы

В качестве формы организации самостоятельной работы применяются методические указания для самостоятельного освоения и приобретения навыков работы со специализированным программным обеспечением. Самостоятельная работа

студентов: изучение теоретического материала; подготовка к лекциям, работа с учебно-методической литературой, подготовка отчётов по 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.

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

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий. Для организации занятий рекомендован онлайн-курс «Б1.О.55.04 Современные технологии защиты информации (10.05.01)», размещенный на платформе Электронного университета ВГУ (LMS moodle), а также Интернет-ресурсы, приведенные в п.15в.5.

18. Материально-техническое обеспечение дисциплины

Учебная аудитория для лекций: специализированная мебель, компьютер преподавателя, мультимедийный проектор, экран.

Учебная аудитория для лабораторных занятий: специализированная мебель, персональные компьютеры, мультимедийный проектор, экран, лабораторное оборудование программно-аппаратных средств обеспечения информационной безопасности.

Аудитория для самостоятельной работы: учебная мебель, компьютер с возможностью подключения к сети «Интернет» и электронной платформе Электронного университета ВГУ.

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

19. Оценочные средства для проведения текущей и промежуточной аттестаций

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

№ п/п	Наименования раздела дисциплины	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Основные понятия безопасности информации и общее состояние информационной безопасности	ОПК-2.2	ОПК-2.2.2	устный опрос, тест, лабораторная работа
2	Основные угрозы информационной и кибербезопасности, их причины и условия возникновения	ОПК-2.2	ОПК-2.2.2	устный опрос, тест, лабораторная работа
		ОПК-2.2	ОПК-2.2.2	
			ОПК-2.2.2	
3	Функции обеспечения безопасности в современной киберсреде	ОПК-2.3	ОПК-2.2.2	устный опрос, тест, лабораторная работа
		ОПК-2.3	ОПК-2.2.2	
			ОПК-2.2.3	
4	Методы нарушения информационной и киберфизической	ОПК-2.3	ОПК-2.2.2	устный опрос, тест, лабораторная работа
			ОПК-2.2.3	

	безопасности			
5	Современные технологии обеспечения информационной и киберфизической безопасности	ОПК-2.3 ОПК-2.3	ОПК-2.3.1 ОПК-2.3.1 ОПК-2.3.1	устный опрос, тест, лабораторная работа
Промежуточная аттестация, форма контроля - экзамен				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,
- курсовая работа

Перечень лабораторных работ

1	Поиск уязвимостей в программном обеспечении	Изучение принципов поиска уязвимостей в программном обеспечении без исходных кодов
2	Эксплуатация уязвимостей	Изучение подходов, применяемых при эксплуатации уязвимостей
3	Аудит безопасности драйверов	Аудит безопасности драйверов режима ядра ОС Windows.
4	Разработка защитных компонентов	Разработка защитных компонентов, функционирующих на уровне ядра ОС Windows
5	Аппаратная виртуализация	Использование технологии аппаратной виртуализации для разработки механизмов защиты ОС
6	Методы защиты программного обеспечения	Изучение методов защиты программного обеспечения
7	Анализ программного обеспечения	Использование инструментария исполняемого кода при анализе программного обеспечения
8	Исследование исполняемых файлов	Изучение методов исследования исполняемых файлов с элементами самозащиты
9	Анализ вредоносного программного обеспечения	Анализ вредоносного программного обеспечения с использованием статических и динамических подходов
10	Методы машинного обучения в средствах защиты	Использование методов машинного обучения в средствах защиты

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

Курсовые работы (примерный перечень тем курсовых работ)

1. Система изучения криптографических алгоритмов.
2. Повышение надежности передачи информации по сети в условиях помех со стороны нарушителя.
3. Разработка системы работы с данными медицинского назначения.
4. Система разделения доступа по ролям.
5. Реализация модели политики доменов и типов.
6. Исследование атак типа PHP-инъекций и методов их предотвращения.
7. Реализация ЭЦП средствами прикладных API операционных систем.
8. Разработка системы распознавания реальных пользователей при аутентификации (CAPTCHA).
9. Исследование методов стеганографии, программная реализация одного из методов.
10. Разработка системы сертификации открытых ключей.
11. Исследование методов защиты программ от несанкционированного запуска.
12. Исследование программных интерфейсов управления доступом к ресурсам ОС. Программная реализация возможности изменения прав доступа произвольной учетной записи или группы к ресурсам системы.
13. Реализация системы аутентификации на основе клавиатурного почерка.
14. Реализация системы распределенной аутентификации типа «запрос-ответ».
15. Исследование методов защиты программ от отладчиков. Программная реализация одного из методов.
16. Реализация асимметричной криптографии средствами прикладных API.
17. Исследование методов обфускации исходного кода.
18. Разработка системы моделирования мандатного доступа к ресурсам ОС.
19.Исследование методов генерации криптостойких случайных чисел с проверкой по тестам FIPS-140.
20. Реализовать один из методов генерации сверхбольших простых чисел с вероятностной проверкой на простоту.
21. Осуществить формирование и верификацию ЭЦП для выбранного файла по ГОСТ 34.10-2012.

Тема курсовой работы может быть предложена обучающимся, должна быть согласована с руководителем и должна соответствовать содержанию (направлению) дисциплины

Критерии оценивания

Для оценивания результатов обучения при выполнении студентом курсовой работы используются следующие показатели:

Знание применяемых в настоящий момент современных технологий защиты данных
Умение применять технологии защиты информации.
Владение навыками построения и реализации алгоритмов защиты информации
Для оценивания результатов выполнения курсовой работы используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».
Для оценивания результатов выполнения курсовой работы используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Соотношение показателей, критериев и шкалы оценивания результатов выполнения курсовой работы:

Показатель оценивания компетенции	Критерии оценивания компетенций	Шкала оценок
Знание применяемых в настоящий момент технологий защиты данных Умение применять технологии защиты информации. Владение навыками построения и реализации алгоритмов защиты информации	В ходе выполнения и защиты курсовой работы обучающийся продемонстрировал отличное знание применяемых в настоящий момент технологий защиты данных, умение применять технологии защиты информации, владение навыками построения и реализации алгоритмов защиты информации. Привел	Отлично

	логичное, доказательное решение некоторой конкретной задачи, проанализировал полученные в ходе ее решения результаты. Курсовая работа оформлена в соответствии с требованиям по оформлению. В соответствии с методикой оценивания оценка за выполнение курсовой работы – 5 баллов.	
Знание применяемых в настоящий момент технологий защиты данных Умение применять технологии защиты информации. Владение навыками построения и реализации алгоритмов защиты информаци	В ходе выполнения и защиты курсовой работы обучающийся продемонстрировал знание применяемых в настоящий момент технологий защиты данных, умение применять технологии защиты информации, владение навыками построения и реализации алгоритмов защиты информаци, Привел решение некоторой конкретной задачи, проанализировал полученные в ходе ее решения результаты. Курсовая работа оформлена в соответствии с требованиям по оформлению. В соответствии с методикой оценивания оценка за выполнение курсовой работы . – 4 балла.	Хорошо
Знание применяемых в настоящий момент технологий защиты данных Умение применять технологии защиты информации. Владение навыками построения и реализации алгоритмов защиты информации	В ходе выполнения и защиты курсовой работы обучающийся показал знание применяемых в настоящий момент технологий защиты данных, умение применять технологии защиты информации. Курсовая работа оформлена с замечаниями. В соответствии с методикой оценивания оценка за выполнение курсовой работы – 3 балла.	Удовлетво-рительно
Знание применяемых в настоящий момент технологий защиты данных Умение применять технологии защиты информации. Владение навыками построения и реализации алгоритмов защиты информации	Обучающийся не справился с выполнением курсовой работы, результаты работы не соответствуют указанным выше критериям. Курсовая работа не оформлена в соответствии с требованиями. В соответствии с методикой оценивания оценка за выполнение курсовой работы составляет менее 3 баллов.	Неудовлет-ворительно

В ходе выполнения курсовой работы обучающийся демонстрирует знания, умения и навыки, полученные в результате освоения дисциплины.

Теоретический блок курсовой работы:

2 балла – теоретический материал соответствует теме курсовой работы, в полном объеме отражает ее (приведены необходимые доказательства);

1 балл - теоретический материал соответствует теме курсовой работы, кратко отражает ее (отсутствуют необходимые доказательства);

0 баллов - теоретический материал не соответствует теме курсовой работы.

Практический блок курсовой работы:
2 балла – приведенная задача отражает применение теоретического материала, ее решение верно и логично описано;
1 балл – приведенная задача отражает применение теоретического материала, но ее решение кратко или содержит ошибки;
0 баллов – задача отсутствует, или приведенная задача не является практическим применением теоретического материала курсовой работы.
Защита курсовой работы:
1 балл – в процессе подготовки к выполнению курсовой работы и ее написания обучающийся продемонстрировал самостоятельность, самоорганизованность, инициативность, ответственность; во время защиты курсовой работы студент показал знание материала курсовой работы, ответил на дополнительные вопросы по теме работы;
0 баллов – во время подготовки к выполнению курсовой работы и ее написания обучающийся проявил неорганизованность, безынициативность, безответственность; во время защиты курсовой работы студент неуверенно отвечал на вопросы по теме работы, допускал ошибки.

Таким образом, максимальное количество баллов, которое обучающий может получить за курсовую работу, равно 5. Критерии выставления оценки («отлично», «хорошо», «удовлетворительно», «неудовлетворительно») за выполнение курсовой работы приведены выше.

Курсовая работа имеет следующую структуру:
- титульный лист;
- содержание;
- текст работы – содержательная часть курсовой работы;
- список литературы;
- приложения (при необходимости).

Содержательная часть курсовой работы представляет собой 2 блока: теоретический (теоретический материал по теме курсовой работы) и практический (применение теории к решению конкретной задачи). В завершении данной части стоит подвести итог выполненной работы (что было изучено и какой результат получен).
Текст работы располагается на одной стороне листа белой бумаги формата А4 по ГОСТ 2.30168 (размер 210 × 297 мм). допускается представлять иллюстрации и таблицы на листах формата не более 420 × 594 мм, должны соблюдаться следующие размеры полей:
- левое - не менее 30 мм;
- правое - не менее 10 мм;
- верхнее - не менее 15 мм;
- нижнее - не менее 20 мм.

Текст работы может быть набран в текстовом редакторе Microsoft Word шрифтом Times New Roman (14 пунктов) через полтора интервала. Абзацный отступ равен 10-17 мм.
На страницах номер проставляют, как правило, сверху по центру. На титульном листе номер не ставится, но включается в общую нумерацию работы. Объем работы составляет 10-20 листов. Количество используемых библиографических источников – не менее 5.
Скрепленная и оформленная надлежащим образом курсовая работа предоставляется обучающимся на проверку преподавателю. В срок, установленный календарным учебным графиком, через 1-3 рабочих дня после предоставления обучающимся работы преподавателю на проверку, происходит защита курсовой работы, в ходе которой обучающийся должен показать уверенное знание материала работы.

20.2 Промежуточная аттестация

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

Перечень вопросов к экзамену (КИМ №1)

1. Основные понятия. Определение безопасности.
2. Группы причин нарушения безопасности компьютерных систем.
3. Особенности современных программно-аппаратных средств как основных причин
4. нарушений ИБ.
5. Особенности современных информационных технологий с точки зрения нарушений ИБ.
6. Состояние правового обеспечения ИБ.
7. Понятие о системе стандартов в области ИБ.
8. Федеральные критерии безопасности США.
9. Единые критерии, их применение в России.
10. Система стандартов ФСТЭК.
11. Понятие о лицензировании деятельности в области ИБ.
12. Понятие о системе сертификации. Системы сертификации в области ИБ, принятые в
13. России.
14. Понятие угроз ИБ. Систематизация угроз. Модель угроз.
15. Понятие разрушающих программных средств (РПС). Виды РПС, их характеристики.
16. Модели РПС.
17. Компьютерные вирусы. Типы вирусов. Структура вируса и способы заражения.
18. Классификация средств защиты от компьютерных вирусов.
19. Модель нарушителя. Классы нарушителей, их характеристики. Модель атак Говарда.
20. Аморосо, Ландвера. Токсономия.
21. Сценарий компьютерной атаки.
22. Функции защиты, их особенности.
23. Виды контроля безопасности. Средства контроля.
24. Понятие безопасности ПО.
25. Методы анализа безопасности ПО. Принципы анализа ПО без исходных кодов.
26. Методы защиты коммерческого ПО.
27. Структура информационных ресурсов.
28. Понятие компьютерных преступлений.
29. Понятие уязвимостей. Систематизация уязвимостей.
30. Ошибки в системе защиты. Недостатки, служащие причиной возникновения уязвимостей.
31. Безопасность операционных систем (ОС).
32. Понятие политики безопасности. Управление доступом.
33. Механизмы контроля доступа к объектам Windows.
34. Аутентификация пользователей в ОС.
35. Криптографические методы защиты информации. Методы криптоанализа.
36. Стеганографическое сокрытие информации.
37. Методы статистического кодирования информации:
38. Методы адаптивного кодирования информации:
39. Методы защиты информации от искажений.
40. Методы надежной передачи данных.
41. Понятие удаленной атаки.
42. Методы обеспечения безопасности в сети Интернет.
43. Защита от угроз типа "отказ в обслуживании".
44. Систематизация технологий защиты, их краткая характеристика.
45. Понятие киберугроз и кибербезопасности, отличие от информационных угроз.
46. Общая схема технологии построения защищенной информационной системы.

Критерии оценки ответов на вопросы экзамена

Для оценивания результатов обучения на экзамене используется – 4-балльная шала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», критерии оценивания приведены ниже.

Оценка «отлично» - студент демонстрирует глубокое понимание темы, умеет распространять вытекающие из теории выводы.
Оценка «хорошо» - студент демонстрирует понимание теоретических положений темы и базовых понятий, но допускает неточности в ответах, испытывает затруднения в применении знаний к анализу состояния проекта.
Оценка «удовлетворительно» - студент отвечает не на все предложенные вопросы, но не менее, чем на половину из них; не демонстрирует способности применения теоретических знаний для анализа ситуаций.
Оценка «неудовлетворительно» - студент демонстрирует непонимание теоретических основ и базовых понятий курса.

Оценка промежуточной аттестации формируется как интегральная оценка по следующей формуле (При округлении оценки используется правило правильного округления. При получении оценки не менее 3 баллов, выставляется «зачтено», менее 3 баллов - «не зачтено». Приэтом, все лабораторные работы должны быть выполнены и защищены

$$Q_{пром\_ат} = 0{,}2Q_{КР1} + 0{,}2Q_{КР2} + 0{,}6Q_{экз}$$

При округлении оценки используется правило правильного округления. При получении оценки не менее 3 баллов, выставляется «зачтено», менее 3 баллов - «не зачтено». При этом, все лабораторные работы должны быть выполнены и защищены.

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

ОПК-4.1. Способен организовывать защиту информации в компьютерных системах и сетях (по областям применения);

1) закрытые задания (тестовые, средний уровень сложности):

1. Какой вид технического канал утечки информации нельзя выделить в отдельный тип, по физической природе носителя сигнала

	Оптический	
	Радиоэлектронный	
	Акустический	
	Материально-вещественный	
	Гидродинамический	

2. Какое из перечисленных ниже определений является истинным?
Зона R2 –…

	остранство вокруг ТСПИ, в пределах которого напряженность электромагнитного поля превышает допустимое (нормированное) значение	
	остранство вокруг ТСПИ, в котором напряженность электромагнитного убывает пропорционально кубу расстояния от ТСПИ	
	яется фиксированной для каждого типа ТСПИ	
	числяется путем умножения значения зоны R1 на коэффициент, заданный производителем	

3. Какой вид радиоэлектронных закладок не содержит в своем составе активных радиокомпонентов?

	диомикрофон	
	довибратор	
	деомикрофон	
	ерный звукосниматель	

– ОПК-4.1.2. знает современные методы, средства и меры по защите информации в компьютерных системах и сетях;

1) Концепция и структура защиты информации не включает в себя
   a) арсенал технических средств защиты информации предприятия, специализирующиеся на решении
   вопросов защиты информации
   b) четко очерченная система взглядов на эту проблему
   c) **значительное число антивирусных средств**
2) Защита информации должна быть
   a) **непрерывной**
   b) неплановой
   c) пассивной
   d) выборочной
3) Система защиты информации должна удовлетворять требованиям
   a) охватывать весь технологический комплекс информационной деятельности
   b) быть разнообразной по используемым средствам
   c) быть открытой для изменения и дополнения мер
   d) быть нестандартной, разнообразной
   e) быть надежной
   f) **все из перечисленного**
   g) ничего из перечисленного
4) К системе безопасности информации предъявляется требование
   a) предоставление пользователю максимальных полномочий, необходимых ему для выполнения порученной работы
   b) предоставление пользователю минимальных полномочий, необходимых ему для выполнения порученной работы
   c) игнорирование попыток несанкционированного доступа
   d) периодическое реагирование на выход из строя средств защиты
5) Система защиты информации может иметь
   a) правовое обеспечение
   b) организационное обеспечение
   c) аппаратно-программное обеспечение
   d) информационное обеспечение
   e) математическое обеспечение
   f) лингвистическое обеспечение
   g) методическое обеспечение
   h) все из перечисленного
   i) ничего из перечисленного
6. Внедрение ложного объекта возможно через протокол
   1. **ARP**
   2. FTP
   3. POP3
   4. IMAP
   5. SMTP
7. Реализация данной угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы.
   1. сканирование сети
   2. угроза выявления пароля
   3. анализ сетевого трафика
   4. **навязывание ложного маршрута**
8. Стандартная форма записи MAC-адреса имеет следующий вид:
   1 6 пар шестнадцатеричных цифр, разделенных дефисами или двоеточиями
   2 4 пары значений от 0 до 255, разделенных точками

3 В виде нескольких символьных имен, разделенными точками, слева направо по возрастанию уровня иерархии

4 4 пары шестнадцатеричных цифр, разделенных точками

9. IP-адрес согласно протоколу IPv4 записывается в следующей форме:

1 6 пар шестнадцатеричных цифр, разделенных дефисами или двоеточиями

2 4 пары десятичных чисел от 0 до 255, разделенных точками

3 В виде нескольких символьных имен, разделенными точками, слева направо по возрастанию уровня иерархии

4 4 пары десятичных чисел от 0 до 65535, разделенных точками

2) открытые задания (тестовые, средний уровень сложности):

1. Существуют ли полностью пассивные радиомикрофоны, не содержащие в своем составе активных компонент? Если существуют. То как они называются и какими средствами могут быть обнаружены?

Примерный ответ

Да, такой тип радиомикрофонов существует, и они называются эндовибраторами. Эндовибратор— переизлучающая пассивная радиозакладка, средство получения акустической информации, у которого отсутствует источник питания, передатчик и микрофон. Проще говоря, эндовибратор — это жучок. Основой его является цилиндрический объемный резонатор, настроенный на внешнее излучение определенной частоты (чаще всего в диапазоне 300 МГц). При этом собственный четвертьволновый вибратор внутри резонатора создает свое поле переизлучения. При ведении разговоров в помещении меняется и собственная резонансная частота эндовибратора, влияющая, в свою очередь, на поле переизлучения, которое становится модулированным акустическими колебаниями. Работать эндовибратор может только тогда, когда он облучается мощным источником на частоте резонатора, поэтому его невозможно обнаружить такими средствами поиска радиозакладок, как нелинейный локатор, индикатор поля и др. Исключение составляет радиомониторинг.

2. Какой вид имеет спектр одиночного радиоимпульса и почему?

Примерный ответ

Для того чтобы исследовать одиночный импульс представим, что этот импульс повторяется с некоторым периодом T и устремим этот период к бесконечности. Расстояние между соседними гармониками в спектре периодического сигнала равно 1/T. Следовательно, для T стремящегося к бесконечности расстояние между гармониками стремится к нулю, т. е. они сливаются. Амплитуды этих гармоник, стремятся к нулю, т. к. интеграл берется только в пределах существования импульса (вне импульса v(t)=0), а T в знаменателе неограниченно возрастает. Таким образом, отдельных гармоник в спектре одиночного импульса не будет. Этот спектр является сплошным (в него входят все частоты).

ОПК-4.2. Способен анализировать защищенность, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности компьютерных систем и сетей (по областям применения);

1) закрытые задания (тестовые, средний уровень сложности):

1. Требование о возмещении убытков в связи с разглашением информации ограниченного доступа не может быть удовлетворено в случае:
   1. несоблюдения пропускного режима
   2. непринятие мер по соблюдению конфиденциальности*
   3. отсутствия пожарной сигнализации
   4. отсутствия инженерных сооружений
2. Разрешать и ограничивать доступ к информации, определять порядок и условия доступа вправе:
   1 президент РФ
   2 гостехкомиссия России
   3 оператор информационной системы
   4 обладатель информации*
3. Основанием для отказа гражданину в допуске к государственной тайне могут являться:
   1. уклонение от воинской службы

2. принадлежность к общественным объединениям
3. имущественное и должностное понижение
4. уклонение от проверочных мероприятий*

4. Степени секретности сведений и их грифы, составляющих государственную тайну:
1. особо секретно, совершенно секретно, секретно
2. очень секретно, неприкосновенно, секретно
3. совершенно секретно, тайно, секретно
4. особой важности, совершенно секретно, секретно*

5. Какую функцию выполняет периферийное устройство:
1. управления работой ЭВМ по заданной программе
2. оперативного сохранения информации
3. ввода и вывода информации*
4. никаких функций не выполняет

6. Средства защиты информации без участия человека называются:
1. законодательные
2. организационные
3. неформальные
4. формальные*

7. К какому виду относится информация, если она представлена на диске:
1. телекоммуникационная
2. документальная*
3. электронная
4. магнитная

8. К какой из составляющих системы защиты информации относится охрана территории и помещений:
1. кадровое обеспечение
2. организационные*
3. программные
4. технические

9. Заражение компьютерными вирусами может осуществляться в процессе:
1. печати на принтере
2. работы с файлами*
3. форматирования дискеты
4. выключения компьютера

10. Основу средств защиты информации составляют средства:
1. формальные
2. неформальные*
3. программные
4. технические

1) Источниками внешних угроз не являются
a) недобросовестные конкуренты
b) преступные группировки и формирования
c) лица административно-управленческого аппарата
d) компьютерные сети

2) Способствует неправомерному овладению конфиденциальной информацией
a) применение нелицензионного ПО
b) несанкционированный доступ
c) приобретение недорогих технических средств
d) доступ сотрудников к сети Интернет

3) Соединения удаленного доступа могут использоваться
a) для получения несанкционированного доступа к организациям
b) для передачи своих персональных данных
c) для проверки имени и пароля
d) все из перечисленного

4) Механизм аутентификации
a) Модем обратного вызова
b) Проверка отпечатков пальцев
c) Генератор случайных чисел
d) Брандмауэр

5) Эффективная антивирусная программ программа осуществляет контроль

a) За серверами и рабочими станциями
b) За пользователем
c) За дисководом
d) За модемом

6. ... – это сетевой сканер.
   1. **NMap**
   2. WireShark
   3. VirtualBox
   4. Linux

7. ... регламентирует процесс передачи и приема во времени, т.е. определяет допустимые моменты начала, конца, повтора передач, точки синхронизации процессов, в которых осуществляется контрольный обмен между процессами, подтверждающими корректность совершенных к этому моменту передач.
   1. **Сеансовый уровень**
   2. Транспортный уровень
   3. Сетевой уровень

8. ... – это программа-анализатор пакетов.
   1. NMap
   2. **WireShark**
   3. VirtualBox
   4. Linux

9. ... определяет информационные порции для передачи за один сеанс, их форматы и способы передачи, а также правила совместного использования физического уровня несколькими процессами.
   1. **Канальный уровень**
   2. Физический уровень
   3. Техническое обеспечение

4. Как называется процесс, вставки анализирующих функций непосредственно в исходный **код** программы, после компиляции и запуска которой вставленные анализирующие функции выполнятся и выдадут результат работы?

	метка кода	
	струментация кода	
	зинг	
	тирование	

5. Какое из перечисленных ниже утверждений является истинным?

	тический анализ кода происходит без реального выполнения исследуемых программ	
	тический анализ кода требует сборки программы из исходных кодов с добавлением санитайзера	
	тический анализ кода не позволяет отслеживать сценарии возникновения ошибок, являющихся следствиями кроссплатформенности	
	тический анализ кода доступен только для интерпретируемых языков	

6. Содержит ли приведенный ниже фрагмент кода ошибки, которые проявятся при его выполнении только на определенной платформе?

```
Object *p = getObject();
int pNum = reinterpret_cast<int>(p);
```

	, не содержит, этот код будет везде работать одинаково корректно	

	держит. Этот код будет корректно работать на праформе x86-64 и не корректно на платформе x86	
	держит. Этот код будет корректно работать на праформе x86 и не корректно на платформе x86-64	
	держит. Этот код не будет корректно работать ни на одной из платформ	

2) открытые задания (тестовые, средний уровень сложности):

3. Что такое динамический анализ кода и для чего он применяется?

Примерный ответ

Динамический анализ кода — анализ программного обеспечения, производящийся при помощи выполнения программ на реальном или виртуальном процессоре (в отличие от статического анализа).

К основным преимуществам динамического анализа кода относят:

- *Возможность проводить анализ программы без необходимости доступа к её исходному коду. Здесь стоит сделать оговорку, так как программы для динамического анализа различают по способу взаимодействия с проверяемой программой (подробнее с этим можно ознакомиться в этой статье). Например, распространён способ проведения динамического анализа путём предварительного инструментирования исходного кода, то есть добавления специального кода в исходный текст приложения для обнаружения ошибок. В этом случае доступ к коду проверяемой программы будет необходим.*
- *Возможность обнаружения сложных ошибок, связанных с работой с памятью: выход за границу массива, обнаружение утечек памяти.*
- *Возможность проводить анализ многопоточного кода непосредственно в момент выполнения программы, тем самым обнаруживать потенциальные проблемы, связанные с доступом к разделяемым ресурсами, возможные deadlock ситуации.*
- *В большинстве реализаций появление ложных срабатываний исключено, так как обнаружение ошибки происходит в момент ее возникновения в программе; таким образом, обнаруженная ошибка является не предсказанием, сделанным на основе анализа модели программы, а констатацией факта ее возникновения.*

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