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

УТВЕРЖДАЮ
заведующий кафедрой
кибербезопасности
информационных систем
С.Л. Кенин

22.03.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.02 Методология исследований и испытаний средств защиты информации

1. Код и наименование направления подготовки/специальности:
10.05.01 Компьютерная безопасность

2. Профиль подготовки / специализация / магистерская программа:
Математические методы защиты информации

3. Квалификация (степень) выпускника: специалист

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: НМС факультета ПММ, протокол № 10 от 15.06.2021
Внесены изменения: протокол УС факультета ПММ, протокол № 8 от 27.02.2024
Рекомендована с изменениями: протокол НМС факультета ПМ, протокол № 5 от 22.03.2024

8. Учебный год: 2024/2025 **Семестр(ы): 8**

9. Цели и задачи учебной дисциплины:

Цель: освоение студентами с методик исследования, оценки и испытаний программных и программно-аппаратных средств защиты информации

Задачи:

– ознакомить студентов с требованиями и мерами по защите информации в информационных системах, обрабатывающих несекретную информацию;

– ознакомить студентов с методиками сертификационных испытаний СЗИ;

– ознакомить студентов с методами выявления разного рода дефектов, уязвимостей и угроз безопасности информационно-программных систем и механизмов их защиты;

– обучить студентов методике исследования угроз безопасности информации в информационной системе и разработке модели угроз;

– обучить студентов методике испытаний автоматизированных систем на безопасность информации.

10. Место учебной дисциплины в структуре ОПОП:

вариативная часть блока Б1. Входные знания в области математического анализа, теории множеств, матричной алгебры, теории вероятностей и математической статистики.

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

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ПК 2	Способен проводить исследования на всех этапах жизненного цикла программных средств в профессиональной деятельности	ПК 2.1	Знает методы и средства планирования и организации исследований и разработок	Знать: базовые понятия теории эксперимента; основные принципы и приемы извлечения информации об объекте в процессе проведения эксперимента; базовые элементы методов планирования эксперимента. Уметь: формировать математическую модель объекта экспериментальных исследований с минимальным количеством переменных; формировать план эксперимента. Владеть практическими навыками:
				разработки математических моделей объекта эксперимента, планирования эксперимента, разработки рабочих методик эксперимента

		ПК 2.2	Знает методы проведения экспериментов и наблюдений, обобщения и обработки информации, полученной в ходе исследований	Знать: основы методов обработки результатов эксперимента с позиций детерминистского и статистического подходов; основополагающие стандарты в области разработки отчетных документов. Уметь: выбирать технические средства экспериментальных исследований; проводить синтез алгоритмов формирования линейных, квазилинейных и нелинейных оценок измеряемых в ходе эксперимента значений физических величин, оптимальных в смысле заданного критерия; строить точечные и интервальные оценки результата эксперимента, представлять его в стандартном виде; проводить анализ результатов эксперимента с использованием методов линейного регрессионного и корреляционного анализа; Владеть практическими навыками: обработки и анализа результатов эксперимента; применения компьютерных технологий в экспериментальных исследованиях
		ПК 2.3	Планирует стадии исследования или разработки в рамках поставленной задачи, выбирает или формирует программную среду для компьютерного моделирования и проведения экспериментов	Знать: основные принципы и приемы извлечения информации об объекте в процессе проведения компьютерного эксперимента. Уметь: формировать математическую модель объекта компьютерного эксперимента; выбирать программную среду для проведения эксперимента и обработки его результатов; формировать план эксперимента, проводить его декомпозицию на отдельные этапы. Владеть практическими навыками: разработки математических моделей объекта, планирования компьютерного эксперимента.
		ПК 2.4	Использует стандартное и оригинальное программное обеспечение, проводит компьютерный эксперимент,	Владеть практическими навыками: использования стандартного и оригинального программного обеспечения для проведения и обработки данных компьютерного эксперимента, анализа и интерпретации результатов компьютерного эксперимента

			составляет его описание и формулирует выводы	сопоставления с данными реального эксперимента и теоретическими выводами.
ПК-3	Способен осуществлять разработку, анализ и обосновывать эффективность применяемых математических методов защиты информации, возникающих при работе программных и программно-аппаратных средств защиты информации при решении профессиональных, исследовательских и прикладных задач.	ПК-3.1	Формирует и применяет аналитическую модель эффективности внедрения средств защиты информации различных классов.	Знать: математические методы защиты информации, возникающих при работе программных и программно-аппаратных средств защиты информации
		ПК-3.3	Анализирует эффективность функционирования программных средств защиты информации.	Уметь:Анализировать эффективность функционирования программных средств защиты информации
		ПК-3.4	Разрабатывает программные алгоритмы, реализующие современные математические методы защиты информации.	Владеть: навыками разработки программных алгоритмов, реализующих современные математические методы защиты информации

12. Объем дисциплины в зачетных единицах/час:

3/108

Форма промежуточной аттестации: зачет

13. Виды учебной работы

Вид учебной работы		Трудоемкость	
		Всего	По семестрам
			8 семестр
Аудиторные занятия		48	48
в том числе:	лекции	16	16
	практические	16	16
	лабораторные	16	16
Самостоятельная работа		60	60
в том числе: курсовая работа (проект)			
Форма промежуточной аттестации		зачет	зачет
Итого:		108	108

13.1 Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн- курса, ЭУМК*
1. Лекции			
1.1	Роль экспериментальных исследований на различных этапах жизненного цикла создания и технических систем	1. Роль и место экспериментальных исследований в процессе разработки, создания и эксплуатации технических систем. Задачи экспериментальных исследований. Классификация экспериментальных исследований. Особенности экспериментальных процедур измерения, контроля, испытаний, технической диагностики. Сочетание экспериментальных исследований и компьютерного моделирования на различных этапах жизненного цикла технических систем. 2. Основные свойства объекта исследования: параметры, факторы, математическая модель. Теория подобия. Условия эксперимента. Технические средства экспериментальных исследований. Измерения, испытания, контроль. Результат эксперимента	https://edu.vsu.ru/course/
1.2	Основы теории измерений	3. Физическая величина, шкала измерения, метод измерения, хранение, условия измерения, воспроизведение и передача единицы измеряемой величины. 4. Погрешность и точность измерения, погрешность и неопределенность. Случайные и систематические погрешности. Правильность, сходимость и воспроизводимость результатов измерений. 5. Постановка задач оценивания результатов многократных измерений с позиций, детерминированного и статистического подходов. Прямые, косвенные, совокупные и совместные измерения. 6. Оценивание погрешностей прямых, косвенных и совместных измерений. Общая схема применения метода наименьших квадратов.	https://edu.vsu.ru/course/
1.3	Контроль, испытания, техническая диагностика	7. Сущность контроля, виды контроля. Виды и категории испытаний. Эффективность процесса испытаний. Сущность и методы технической диагностики.	https://edu.vsu.ru/course/

1.4	Организация процессов экспериментальных исследований и испытаний	8. Структура организационно-технической системы экспериментальных исследований и испытаний. Экспериментальные исследования с применением методов физического и математического моделирования. Элементы планирования эксперимента. Оптимизация многоэтапных испытаний. 9. Подготовительный этап экспериментальных исследований. Программа и методика эксперимента. Проведение экспериментальных исследований. Воспроизведение и контроль условий эксперимента. Технические и программные средства. 10. Обработка результатов эксперимента. Анализ и интерпретация результатов экспериментов и математического моделирования. Разработка итоговых документов (протокол, акт, отчет). Стандарты в области измерений, испытаний и технической диагностики	
2. Лабораторные занятия			
2.1	Основы теории измерений	1. Формирование оценок измеряемой величины по данным многократных измерений, минимизирующих взвешенные критерии квадратичного вида. Вычисление средних гармонических, геометрических, арифметических и квадратических. Квазилинейные оценки. 2. Формирование робастных оценок, минимизирующих модульный и минимаксный критерии. 3. Построение интервальной оценки измеряемой величины по данным статистических измерений для заданного уровня доверительной вероятности. Представление результатов измерений в стандартном виде. 4. Оценивание результатов прямых измерений в присутствие систематических погрешностей. 5. Определение погрешности косвенных измерений. 6. Обработка результатов совместных (совокупных) измерений методом наименьших квадратов. 7. Построение эмпирических законов распределения результатов эксперимента. Идентификация законов распеределения.	
2.2	Контроль, испытания, техническая диагностика	8. Диагностические методы получения оценок, основанные на применении алгебраических инвариантов	
2.3	Организация процессов экспериментальных исследований и испытаний	9. Разработка методики эксперимента по контролю технических параметров изделия. 10. Формирование протокола измерений.	

13.2 Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Роль экспериментальных исследований на различных этапах жизненного цикла создания и технических систем	4	0	0	16	20
2	Основы теории измерений	6	2	10	36	54
3	Контроль, испытания, техническая диагностика	2	2	2	8	12
4	Организация процессов экспериментальных исследований и испытаний	6	4	4	12	22
	Итого:	16	16	16	60	108

14. Методические указания для обучающихся по освоению дисциплины:

Работа с конспектами лекций, выполнение лабораторных заданий, заданий текущей и промежуточной аттестаций.
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	Сергеев, А. Г. Метрология, стандартизация и сертификация: [учебник и практикум] / А.Г. Сергеев, В. В. Терегеря; - 2-е изд., перераб. и доп. - Москва: Юрайт, 2015. - 838 с.: ил. - ISBN 978-5-9916-4632-1
2	Сергеев, А. Г. Метрология, стандартизация и сертификация: учебник для вузов / А.Г. Сергеев, В.В. Терегеря.- М.: Юрайт, 2010.- 820 с. : ил., табл. - (Основы наук).- Библиогр.: с.815-820 .- ISBN 978-5-9916-0160-3.- ISBN 978-5-9692-0247-4

б) дополнительная литература:

№ п/п	Источник
1	Афанасьева Н.Ю. Вычислительные и экспериментальные методы научного эксперимента: учебное пособие/: учебное пособие / Н.Ю. Афанасьева – М.: КНОРУС,
	2010. – 336 с. – ISBN 978-5-406-00176-9
2	Мурашкина Т. И. Техника физического эксперимента и метрология : [учебное пособие/ Т.И. Мурашкина. – Санкт-Петербург: Политехника, 2015. – 137, [1] с.: ил., табл. – (Учебное пособие для вузов). – Библиогр.: с.137–[138]. – ISBN 978-5-7325-1051-5
3	Гольдштейн А.Е. Физические основы получения информации: учебник / А.Е. Гольдштейн. – Томск: Изд-во Томского политехнического университета, 2010. – 292 с. – ISBN 978-5-98298-650-4
4	Springer Handbook of Metrology and Testing. – Berlin, Heidelberg: Springer-Verlag, 2011. – 1229 p.

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

№ п/п	Ресурс
1	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
2	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)
3	ЭБС Лань – Лицензионный договор №3010-14/37-23 от 07.03.2023 (срок предоставления с 12.03.2023 по 11.03.2024)
4	ЭБС «Университетская библиотека online» – Контракт №3010-06/23-22 от 30.12.2022(срок предоставления с 12.01.2023 по 11.01.2024)

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Сергеев, А. Г. Метрология, стандартизация и сертификация: учебник для вузов / А.Г. Сергеев, В.В. Терегеря . – М.: Юрайт, 2010.— 820 с.: ил., табл. – (Основы наук). – Библиогр.: с.815-820. – ISBN 978-5-9916-0160-3.— ISBN 978-5-9692-0247-4
2	Мироновский Л.А. Функциональное диагностирование динамических систем / Л.А. Мироновский. – М.: Изд-во МГУ, 1998. – 254 с.
3	Демина Л.Н. Методы и средства измерений, испытаний и контроля: учебное пособие. – М.: НИЯУ МИФИ, 2010. – 292 с.

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

При реализации дисциплины используются модульно-рейтинговая и личностно-ориентированные технологии обучения (ориентированные на индивидуальность студента, компьютерные и коммуникационные технологии). В рамках дисциплины предусмотрены следующие виды лекций: информационная, лекция-визуализация, лекция с применением обратной связи.

Дисциплина реализуется с применением электронного обучения и дистанционных образовательных технологий, для организации самостоятельной работы обучающихся используется онлайн-курс, размещенный на платформе Электронного университета ВГУ (LMS moodle), а также другие Интернет-ресурсы, приведенные в п.15в

18. Материально-техническое обеспечение дисциплины (см.файл мто):

Лекционная аудитория должна быть оборудована учебной мебелью, компьютером, мультимедийным оборудованием (проектор, экран, средства звуковоспроизведения), допускается переносное оборудование.

Лабораторные занятия должны проводиться в специализированной аудитории, оснащенной учебной мебелью и персональными компьютерами с доступом в сеть Интернет (компьютерные классы, студии), мультимедийным оборудованием (мультимедийный проектор, экран, средства звуковоспроизведения). Число рабочих мест в аудитории должно быть таким, чтобы обеспечивалась индивидуальная работа студента на отдельном персональном компьютере.

Для самостоятельной работы необходимы компьютерные классы, помещения, оснащенные компьютерами с доступом к сети Интернет.

Программное обеспечение:
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	Наименование раздела дисциплины (модуля)	Компетенция	Индикатор достижения компетенции	Оценочные средства
1	Разделы 1-4 Роль экспериментальных исследований на различных этапах жизненного цикла создания и технических систем. Основы теории измерений. Контроль,испытания, техническая диагностика. Организация процессов экспериментальных исследований и испытаний	ПК 2	ПК 2.1, ПК 2.2, ПК 2.3	Контрольные работы по соответствующим разделам и темам. Задания и отчеты о выполнении лабораторных работ 1-10
		ПК 3	ПК 3.1, ПК 3.3, ПК 3.4	
Промежуточная аттестация форма контроля – зачет				Перечень вопросов в виде комплекта КИМ, перечень заданий для выполнения лабораторных работ

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах: устного опроса; защиты лабораторных работ, выполнения контрольных работ.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования. Промежуточная аттестация по итогам освоения дисциплины проводится в форме зачета с оценкой и экзамена. Для получения положительной итоговой оценки необходимо выполнение всех лабораторных и контрольных работ.

20.1. Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью лабораторных и контрольных работ.

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины, осуществляется в ходе текущей и промежуточной аттестаций.

Промежуточная аттестация включает в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и результаты выполнения лабораторных работ, позволяющие оценить степень сформированности умений и навыков.

Для оценивания результатов обучения на зачете используется – зачтено, не зачтено

Соотношение показателей, критериев и шкалы оценивания результатов обучения.

Примерный перечень и порядок использования оценочных средств

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
	Устный опрос	Вопросы по темам/разделам дисциплины	Правильный ответ – зачтено, неправильный или принципиально неточный ответ – не зачтено

	Контрольная работа по разделу дисциплины	Теоретические вопросы темам/разделам дисциплины	Шкала оценивания соответствует приведенной в
	Лабораторная работа	Содержит четыре лабораторных задания, предусматривающих выполнение типовых операций по организации, планированию и обработке результатов эксперимента	При успешном выполнении работ в течение семестра фиксируется возможность оценки только теоретической части дисциплины в ходе промежуточной аттестации, в противном случае проверка задания по лабораторным работам выносится на зачет

20.2 Промежуточная аттестация

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины, осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах: устного опроса, практических заданий. Критерии оценивания приведены выше.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Контрольно-измерительные материалы промежуточной аттестации включают в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и практическое задание, позволяющее оценить степень сформированности умений и навыков по управленческой деятельности на проектах.

При оценивании используются качественные шкалы оценок. Критерии оценивания приведены выше.

Примерный перечень вопросов

№ п/п	Содержание
1	Роль и место экспериментальных исследований в процессе разработки, создания и эксплуатации технических систем
2	Задачи экспериментальных исследований. Классификация экспериментальных исследований
3	Особенности экспериментальных процедур измерения, контроля, испытаний, технической диагностики
4	Физическая величина. Понятие измерения
5	Шкала измерения. Типы шкал
6	Понятие метода измерения. Классификация измерений
7	Условия измерения. Нормальные, рабочие, предельные условия. Хранение, воспроизведение и передача единицы измеряемой величины
8	Понятия погрешности и точности измерения. Классификация погрешностей
9	Погрешность и неопределенность. Сравнительный анализ двух подходов к выражению точности измерений
10	Качество измерений: правильность, сходимость и воспроизводимость
11	Постановка задач оценивания результатов многократных измерений с позиций детерминистского подхода
12	Постановка задач оценивания результатов многократных измерений с позиций статистического подхода
13	Точечные и интервальные оценки результатов многократных прямых измерений. Представление результата в стандартном виде
14	Оценивание точности измерений в присутствии систематических погрешностей. Суммарная погрешность

15	Оценивание погрешностей косвенных измерений
16	Равноточные и неравноточные измерения. Вес. Объединение результатов измерений
17	Совокупные и совместные измерения. Применение метода наименьших квадратов
18	Сущность контроля, виды контроля
19	Виды и категории испытаний. Эффективность процесса испытаний
20	Оптимизация многоэтапных испытаний
21	Сущность и методы технической диагностики
22	Структура организационно-технической системы экспериментальных исследований и испытаний
23	Экспериментальные исследования с применением методов физического и математического моделирования
24	Подготовительный этап экспериментальных исследований. Программа и методика эксперимента
26	Проведение экспериментальных исследований. Воспроизведение и контроль условий эксперимента
27	Технические и программные средства. Выбор, метрологический контроль
28	Обработка результатов эксперимента. Типовые процедуры
29	Разработка итоговых документов (протокол, акт, отчет)
30	Стандарты в области измерений и испытаний

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

Какие подходы могут применяться при построении системы управления кибербезопасностью организации? Выберите все правильные ответы.

- Вероятностный
- Директивный
- **Регуляторный**
- **Риск-ориентированный**
- Технологический
- Объектный

2 Какие из перечисленных киберугроз являются ключевыми на ближайшее будущее? Выберите все правильные ответы.

- **Устройства IoT как площадка для реализации атак**
- Спам
- **Программы-вымогатели**
- **Criminal-as-a-service (переход киберпреступников на сервисную модель)**
- Программы-шпионы
- **«Призраки интернета прошлого» (угрозы от устаревшего программного и программно-аппаратного обеспечения, которое находится в интернете)**
- Программы-майнеры
- Скимминг

3 Что из нижеперечисленного является тенденциями сетевой информационной безопасности? Выберите все правильные ответы.

- Установка накладных средств защиты на сетевые устройства
- **Интеграция с решениями по расследованию сетевых инцидентов**
- **Инспектирование зашифрованного трафика**
- Развитие общего сетевого периметра
- **Интеграция с Threat Intelligence**
- Уход от использования виртуальных и облачных межсетевых экранов
- **Мониторинг аномалий во внутренней сети**
- Внедрение протокола TLS 1.1 для защиты веб-трафика

4. Является ли "обеспечение контроля целостности средств защиты и немедленное реагирование на их выход из строя" требованием к системе безопасности?

- Нет.
- **Да.**
- Да, при определенных настройках параметров системы.
- Нет, поскольку это - функции любой операционной системы.

5. Является ли "определение полномочий и прав пользователей на доступ к определенным видам информации" требованием к системе безопасности?
- Да, при определенных настройках параметров системы.
- Нет.
- Нет, поскольку это - функции любой операционной системы.
- **Да.**

6. Является ли "разнообразие используемых средств" требованием к системе безопасности?
- **Нет.**
- Да.
- Да, при определенных настройках параметров системы.
- Нет, поскольку это - функции любой операционной системы.

7. Является ли "простота технического обслуживания и удобство эксплуатации пользователями" требованием к системе безопасности?
- Да, при определенных настройках параметров системы.
- **Нет.**
- Нет, поскольку это - функции любой операционной системы.
- Да.

8. Является ли "предоставление пользователю минимальных полномочий, необходимых ему для выполнения порученной работы" требованием к системе безопасности?
- Да, при определенных настройках параметров системы.
- **Да.**
- Нет, поскольку это - функции любой операционной системы.
- Нет.

9. Является ли "учет случаев и попыток несанкционированного доступа к конфиденциальной информации" требованием к системе безопасности?
- **Да.**
- Нет.
- Да, при определенных настройках параметров системы.
- Нет, поскольку это - функции любой операционной системы.

10. Является ли "обеспечение оценки степени конфиденциальности информации" требованием к системе безопасности?
- Нет.
- **Да.**
- Да, при определенных настройках параметров системы.
- Нет, поскольку это - функции любой операционной системы.

1. Системы анализа уязвимостей позволяют:

а) выявить злоумышленника, работающего в компьютерной сети;

б) выявить уязвимости проектируемой системы защиты информации; *в) выявить уязвимости действующей системы защиты информации.*

2. Использование электронной подписи позволяет не допустить (лишнее исключить):

а) отказ от авторства;

б) приписывание авторства;

в) несанкционированное ознакомление с подписанным документов.

3. Что такое несанкционированный доступ (нсд)?

1) Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа

2) Создание резервных копий в организации

3) Правила и положения, выработанные в организации для обхода парольной защиты

4) Вход в систему без согласования с руководителем организации

5) Удаление не нужной информации

4. В чем заключается основная причина потерь информации, связанной с ПК?

1) с глобальным хищением информации

2) с появлением интернета

3) с недостаточной образованностью в области безопасности

5. Открытость для изменения и дополнения мер обеспечения безопасности информации - это общее требование к защите информации (1) или требование, предъявляемое к системе безопасности информации (2), или условие, которому должна удовлетворять система защиты информации (3)?

- (1).
- (2).
- **(3).**
- Ни одно из этих понятий.

6. Нестандартность, разнообразность - это общие требования к защите информации (1) или требование, предъявляемое к системе безопасности информации (2), или условие, которому должна удовлетворять система защиты информации (3)?

- (1).
- (2).
- **(3).**
- Ни одно из этих понятий.

7. Комплексность - это общие требования к защите информации (1) или требование, предъявляемое к системе безопасности информации (2), или условие, которому должна удовлетворять система защиты информации (3)?

- **(1).**
- (2).
- (3).
- Ни одно из этих понятий.

8) Программные закладки могут выполнять действия

a) вносить произвольные искажения в коды программ

b) переносить фрагменты информации

c) искажать выводимую информацию

d) Все из перечисленного

e) Ничего из перечисленного

9) Угрозами конфиденциальной информации не являются

a) ознакомление без нарушения ее целостности

b) модификация информации

c) разрушение информации

d) создание и распространение вирусов

10) Вредоносный код проникает в организации способами

a) Файлы с общим доступом с домашних и рабочих компьютеров

b) Файлы, загружаемые с сайтов интернета

c) Файлы, поступающие в организацию в виде вложений электронной почты

d) Файлы, внедряемые в системы посредством использования уязвимостей

e) Все из перечисленного

f) Ничего из перечисленного

11. Какую опасность представляют open-source библиотеки и инструменты в корпоративной среде? Выберите все правильные ответы.

1. **Часто отсутствуют механизмы аутентификации**
2. **Присутствуют избыточные права и повышение привилегий**
3. Используются нестандартные сетевые протоколы
4. **Встречаются незаблокированные стандартные учетные записи**
5. Не допускается сканирование антивирусом
6. **В конфигурационных файлах встречаются пароли в открытом виде**

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) 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

3) 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

4) 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

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

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

7. Где применяются средства контроля динамической целостности?
1. анализе потока финансовых сообщений
2. обработке данных
3. при выявлении кражи, дублирования отдельных сообщений

8. Укажите, какую модель информационной безопасности приводят в качестве стандартной:
(1) конфиденциальность, подлинность, достоверность
(2) конфиденциальность, целостность, доступность
(3) достоверность, целостность, доступность
(4) апеллируемость, целостность, доступность

9. Укажите, какой процесс тестирования проверяет соответствие функционирования продукта его начальным спецификациям:
(1) тестирование пользовательского интерфейса
(2) тестирование удобства использования
(3) функциональное тестирование
(4) нагрузочное тестирование
(5) тестирование безопасности

10. Укажите, приложением какого языка разметки является HTML:
(1) OWL
(2) SGML
(3) XML
(4) XHTML

11. Укажите, каким утверждением нельзя охарактеризовать централизованную архитектуру:
(1) пользователи совместно используют дорогие ресурсы хост-ЭВМ и дорогие периферийные устройства
(2) централизация ресурсов и оборудования облегчает обслуживание и эксплуатацию вычислительной системы
(3) присутствует необходимость администрирования рабочих мест пользователей
(4) пользователи полностью зависят от администратора хост-ЭВМ.

Что из нижеперечисленного является тенденциями хостовой информационной безопасности?

Выберите все правильные ответы.

- **Сдвиг в сторону EDR-решений**
- Применение узкоспециализированных решений
- **Использование локальной и облачной песочницы для анализа подозрительных файлов**
- **Обмен данными и командами с решениями по защите сетевых устройств**
- Избегание SAAS-модели как несущей повышенные риски с точки зрения ИБ
- Выбор в пользу единственного корпоративного антивируса и antimalware-движка

2 Что из нижеперечисленного является тенденциями Identity & Access Management? Выберите все правильные ответы.

- **Более эффективное управление привилегированными пользователями**
- Внедрение однофакторной аутентификации
- Отказ от использования софт-токенов в пользу биометрии
- **Интеграция со средствами защиты IPS и SIEM**
- **Контроль поведения пользователей с помощью технологии UEBA**
- Внедрение локальной аутентификации

3 Какой способ начала кибератаки самый распространенный в настоящее время?

- Подбор пароля по словарю
- **Фишинг**
- Сканирование портов
- Перехват сетевого трафика

4 В чем особенность кибератак с применением вирусов-шифровальщиков, начиная с 2020?

- Выкуп для расшифрования данных запрашивается неоднократно
- Не всегда удается расшифровать данные
- **Перед шифрованием предпринимается попытка похитить конфиденциальную информацию**
- Вирус-шифровальщик распространяется по сети, используя незакрытые уязвимости

5 Какой подход наиболее эффективен в обеспечении кибербезопасности устройств интернета вещей?

- Установка антивируса на устройства IoT
- Физическая безопасность
- Назначение сложных паролей
- **Поведенческий анализ на основе моделей машинного обучения**

6. Подмена доверенного объекта сети реализуется в системах, где применяются … алгоритмы идентификации и аутентификации хостов, пользователей

1. **Нестойкие**
2. Стойкие
3. Полиморфные
4. Инкапсулированные
5. Распределенные

7. Угроза типа «Анализ сетевого траффика» реализуется с помощью специальной …

1. **программы-анализатора пакетов**
2. утилиты межсетевого взаимодействия
3. операционной системы
4. СУБД

8. Какая из перечисленных моделей применяется для описания хакерских группировок?

1. Kill Chain
2. MITRE ATT&CK
3. **Diamond Model**
4. OWASP Top 10

9. Продолжите утверждение: главный постулат DATA-DRIVEN состоит в том, что решения нужно принимать, опираясь на…

1. **Анализ данных, а не интуицию и личный опыт**
2. Результаты анализа AI
3. Усредненную экспертную оценку
4. Результаты статистических исследований

10. К какой категории информации CTI следует отнести сведения о техниках атаки?

1. Технической
2. **Тактической**
3. Операционной
4. Стратегической

1. Несанкционированный доступ (НСД) к информации:

а) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС);

б) доступ к информации, нарушающий установленные правила разграничения доступа, с использованием специально разработанных технических средств;

в) копирование, искажение или модификация информации с нарушением установленных правил разграничения доступа.

2. Блокирование персональных данных:

а) временное прекращение обработки персональных данных;

б) действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

в) действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

3. Обезличивание персональных данных:

а) действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

б) действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных;

в) все перечисленные действия.

4. Свойство открытости означает, что система реализует открытые спецификации, достаточные для того, чтобы обеспечить:

1. возможность переноса разработанного прикладного программного обеспечения на широких диапазон систем с минимальными изменениями (мобильность приложений, переносимость)
2. совместную работу (взаимодействие) с другими прикладными приложениями на локальных и удаленных платформах (интероперабельность, способность к взаимодействию)
3. взаимодействие с пользователями в стиле, облегчающим последним переход от системы к системе (мобильность пользователей)
4. **все вышеперечисленное**

5. Шифр, который представляет собой последовательность (с возможным повторением и чередованием) основных методов преобразования, применяемую к части шифруемого текста, называется

A) блочный
B) рассечение-разнесение
C) подстановка
D) гаммирование

6. Шифр, который заключается в том, что массив защищаемых данных делится на такие элементы, каждый из которых в отдельности не позволяет раскрыть содержание защищаемой информации, и которые хранятся по разным зонам ЗУ или располагаются на различных носителях, называется

A) рассечение-разнесение
B) блочный
C) гаммирование
D) перестановка

7) Парольная аутентификация имеет достоинство

a) Простота и удобства для человека
b) Наложение технических ограничений (длина пароля, алфавит пароля)
c) Управление сроком действия пароля, их периодическая смена
d) Ограничение доступа к файлу паролей
e) Ограничение числа неудачных попыток входа в систему
f) Обучение пользователей

8) Ролевое управление предполагает

a) Опрос пользователя

b) Для каждого пользователя активны несколько ролей
c) Проверку отпечатков пальцев
d) Проверку геометрии руки и лица

9) Ролевое управление не определяется понятием
a) Пользователь
b) Сеанс работы пользователя
c) Роль (определяемая организационной структурой)
d) Должность
e) Объект (сущность, доступ к которой разграничивается)
f) Операция (выполняемая над объектом)
g) Право доступа

10. Какие атаки предпринимают хакеры на программном уровне?
1) атаки на уровне ОС
2) атаки на уровне сетевого ПО
3) атаки на уровне пакетов прикладных программ
4) атаки на уровне СУБД

11. Утечка информации
1) несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу
2) ознакомление постороннего лица с содержанием секретной информации
3) потеря, хищение, разрушение или неполучение переданных данных

1. Укажите, какой элементы серверной архитектуры AJAX позволяет клиентскому сценарию JavaScript получать и задавать свойства для пользователя, связанного с текущим запросом:
(1) пользовательские Веб-службы
(2) методы страниц
(3) служба проверки подлинности
(4) служба ролей
(5) служба профилей
(6) JSON-сериализация

2. Укажите действия, из которых состоят все операции запроса LINQ:
(1) получение источника данных, выполнение запроса
(2) создание запроса, выполнение запроса
(3) получение источника данных, создание запроса, выполнение запроса
(4) получение данных, создание запроса, выполнение запроса

3. JavaScript - это:
(1) объектно-ориентированный язык программирования
(2) скриптовый язык программирования, обладающий свойствами объектно-ориентированного языка
(3) процедурный язык программирования
(4) функциональный язык программирования

4. JSON - это:
(1) текстовый формат обмена данными, основанный на XML
(2) текстовый формат обмена данными, основанный на JavaScript
(3) текстовый формат обмена данными, основанный на HTML
(4) текстовый формат обмена данными, основанный на CSS

5. Укажите, какой элемент уровня связи Веб-служб выполняет асинхронные сетевые запросы:
(1) WebRequest
(2) WebRequestManager
(3) XmlHttpExecutor
(4) JSON-сериализация

6. Укажите, каким утверждением нельзя охарактеризовать RIA-приложение:
(1) передает веб-клиенту необходимую часть пользовательского интерфейса, оставляя большую часть данных на сервере
(2) требует хранения части данных на жестком диске
(3) запускается в браузере
(4) запускается локально в среде безопасности, называемой "песочница"

7. MSF состоит из:
(1) двух моделей и двух дисциплин
(2) двух моделей и трех дисциплин
(3) трех моделей и трех дисциплин

(4) двух моделей и пяти дисциплин

8. С появлением CSS стало возможным разделение:

(1) содержания и разметки

(2) стилей и представления

(3) содержания и представления

(4) содержания и скриптов

9. Укажите, какой признак не относится к базам данных:

(1) база данных хранится и обрабатывается в вычислительной системе

(2) данные в базе данных логически структурированы

(3) база данных включает метаданные

(4) все признаки относятся к базам данных

10. Укажите свойство не присущее JavaScript:

(1) все идентификаторы зависят от регистра

(2) в названиях переменных можно использовать буквы, подчеркивание, символ доллара, арабские цифры

(3) названия переменных могут начинаться с буквы или цифры

(4) для оформления однострочных комментариев используются //

1) При использовании паролей следует руководствоваться

a) Длинной пароля

b) Частотой смены пароля

c) Историей пароля

d) Содержимым пароля

e) Все из перечисленного

f) Ничего из перечисленного

2) ISO 17799 не охватывает

a) Политику безопасности

b) Организационная безопасность

c) Классификация и контроль имущества

d) Безопасность персонала

e) Физическая безопасность и безопасность среды

f) Управление коммуникациями и операциями

g) Контроль доступа

h) Разработка и поддержка систем

i) Поддержка непрерывности деловых процессов

j) Соответствие политике

k) Охватывает все

3) Что является инженерно-технической формой защиты информации:

а) разработка и реализация специальных законов, нормативно-правовых актов, правил и юридических процедур, обеспечивающих правовую защиту информации;

б) регламентация производственной деятельности и взаимоотношений персонала, направленная на защиту информации;

в) использование различных технических, программных и аппаратных средств защиты информации от несанкционированного доступа, копирования, модификации или уничтожения.

4) К числу определяющих признаков, по которым производится классификация информационных систем, относятся:

а) наличие в информационной системе информации различного уровня конфиденциальности;

б) уровень значимости информации и масштаб информационной системы;

в) режим обработки данных в информационной системе - коллективный или индивидуальный.

5. Какой нормативный документ является приоритетным в РФ

А) Федеральные законы РФ

Б) Международные акты

В) Постановления Правительства РФ

Г) Указы президента РФ

6. Какая информация подлежит защите?

А) информация, циркулирующая в системах и сетях связи

Б) зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать

В) только информация, составляющая государственные информационные ресурсы

Г) любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу

7. Объект защиты информации это…

А) информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности

Б) информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации

В) объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности

Г) информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

8. Как называется доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами?

- мандатный доступ;
- атака;
- **несанкционированный доступ.**

9. Как называется способ защиты информации от утечки через ПЭМИН, основанный на локализации электромагнитной энергии в определенном пространстве за счет ограничения распространения ее всеми возможными способами?

- **экранирование;**
- подавление;
- зашумление.

10. Как называются методы защиты акустической информации, предусматривающие подавление технических средств разведки?

- пассивные;
- **проактивные;**
- **активные.**

11. Укажите, какой вид атаки возникает, когда Веб-сервер позволяет атакующему получать доступ к важной информации или функциям, доступ к которым должен быть ограничен:

(1) предсказуемое значение идентификатора сессии

(2) недостаточная авторизация

(3) отсутствие таймаута сессии

(4) фиксация сессии

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