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.14 Основы инженерно-технической защиты информации

1. Код и наименование направления подготовки/специальности:

10.05.01. Компьютерная безопасность

2. Профиль подготовки / специализация / магистерская программа:

Безопасность компьютерных систем и сетей

3. Квалификация (степень) выпускника: специалист

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: кибербезопасности информационных систем

6. Составители программы: Кенин Сергей Леонидович кандидат технических наук, доцент

7. Рекомендована: НМС факультета ПММ, протокол № 5 от 22.03.2024

_____
_____

отметки о продлении вносятся вручную)

8. Учебный год: 2026/2027 **Семестр(ы): 5**

9. Цели и задачи учебной дисциплины:

Целями и задачами дисциплины является ознакомление студентов с принципами работы и характеристиками современных инженерно-технических средств защиты информации; техническими каналами утечки информации; поиском и обнаружением ТКУИ; формированием требований по защите информации; методами расчета и контроля показателей технической защиты информации; оптический (визуальный) канал утечки информации; техника перехвата телефонных разговоров. Формирование знаний и навыков у студентов об основных методах и технологиях обеспечения информационной безопасности в прикладных системах, об обеспечении защиты от несанкционированного доступа и сетевых хакерских атак; о применении средств по выбору лучшего способа обеспечения защиты информации с применением современного ПО
Форма(ы) промежуточной аттестации - зачет с оценкой, курсовой проект.

10. Место учебной дисциплины в структуре ОПОП:

Место учебной дисциплины в структуре ОПОП: вариативная часть блока Б1.

Дисциплина связана с другими дисциплинами образовательной программы: «Основы информационной безопасности», «Операционные системы», «Аппаратные средства вычислительной техники». Дисциплины, для которых освоение данной дисциплины необходимо как предшествующее: «Защита информации от утечки по техническим каналам», «Научно-исследовательская работа», «Проектно-технологическая практика», «Преддипломная практика».

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

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ПК-1	Способен проводить анализ требований и выполнять работы по проектированию программных и аппаратных компонент системы безопасности компьютерных систем и сетей, в том числе с использованием современных методов и средств защиты информации	ПК-1.3	Использует принципы комплексной разработки правил, процедур, приемов и методов, при создании средств защиты информации, в том числе с использованием современных методов и средств разработки программного обеспечения	**знать:** принципы комплексной разработки правил, процедур, приемов и методов, **уметь:** использовать принципы комплексной разработки правил, процедур, приемов и методов, при создании средств защиты информации **владеть:**. навыками использованием современных методов и средств разработки ПО

ПК-2	Способен принимать участие в экспертизе и анализе уязвимостей, угроз и инцидентов информационной безопасности в компьютерных системах и сетях	ПК-2.2	способен проводить анализ компьютерных систем с целью определения уровня защищённости и доверия с последующим обобщением и обработкой информации, полученной в ходе исследований	**знать:** принципы анализа компьютерных систем с целью определения уровня защищённости и доверия **уметь:** проводить анализ компьютерных систем с целью определения уровня защищённости и доверия с последующим обобщением и обработкой информации **владеть:**.методами анализаа КС, определять уровень защищенности ,обрабатывать и обобщать информацию, полученную в ходе исследований
		ПК-2.3	– использует типовое и специализированное программное обеспечение для оценки рисков, связанных с осуществлением угроз безопасности в отношении компьютерной системы	**знать:** возможности использования специализированного ПО **уметь:** использовать типовое и специализированное программное обеспечение **владеть:** навыками работы со специализированным ПО
ПК-3	Способен участвовать в работах по проектированию систем защиты информации в компьютерных системах и сетях при решении профессиональных, исследовательских и прикладных задач	ПК-3.4	– способен проводить анализ и формализацию поставленных задач в области безопасности компьютерных систем и сетей	**знать:** методы проведения анализа и формализации поставленных задач в области ИБ **уметь:** проводить анализ и формализацию поставленых задач **владеть:** практическими навыками проведения анализа в области ИБ КС
		ПК-3.6	– способен участвовать в проектировании системы защиты информации и подсистем информационной безопасности компьютерной системы	**знать:** основы проектирования систем и подсистем **уметь:** проектировать системы защиты информации и подсистем информационной безопасности компьютерной системы **владеть:п**рактическими навыками проектирования систем защиты информации

12. Объем дисциплины в зачетных единицах/час — 4/144. **Форма промежуточной аттестации:** зачет с оценкой, курсовой проект

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			№ семестра 5	№ семестра	Итого
Аудиторные занятия		80	80		80
в том числе:	лекции	32	32		32
	практические	-	-		-
	лабораторные	48	48		48
Самостоятельная работа		64	64		64
в том числе: курсовая работа (проект)					
Форма промежуточной аттестации *(зачет – час. / экзамен – час.)*					
Итого:		144	144		144

13.1 Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью он-лайн-курса, ЭУМК
1. Лекции			
1.1	Концепция инженерно-технической защиты информации	Общие представления о защищаемой информации Демаскирующие признаки объектов защиты	https://edu.vsu.ru/course/view.php?id=16568
1.2	Теоретические основы инженерно-технической защиты информации	Виды угроз и способы добывания защищаемой информации	https://edu.vsu.ru/course/view.php?id=16568
1.3	Физические основы защиты информации	Каналы утечки информации при эксплуатации ЭВМ	https://edu.vsu.ru/course/view.php?id=16568
1.4	Технические средства добывания и инженерно-технической защиты информации	Классификация и структура технических каналов утечки информации Системы контроля управления доступом Системы противопожарной сигнализации	https://edu.vsu.ru/course/view.php?id=16568
1.5	Организационные основы инженерно-технической защиты информации	Разработка систем инженерно-технической защиты информации	https://edu.vsu.ru/course/view.php?id=16568
1.6	Методическое обеспечение инженерно-технической защиты информации	Разработка систем инженерно-технической защиты информации	https://edu.vsu.ru/course/view.php?id=16568
2. Практические занятия			

2.1	нет		
3. Лабораторные работы			
3.1	Системы контроля и управления доступом (СКУД)	Виды штрих-кодов и считывание. Построение системы контроля управления доступом на базе контактных смарт-карт, на базе биометрических систем, с использованием видеофиксации	https://edu.vsu.ru/course/view.php?id=16568

13.2 Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные	Сам. работа	Всего
1.1	Концепция инженерно-технической защиты информации	4		8	12
1.2	Теоретические основы инженерно-технической защиты информации	4		8	12
1.3	Физические основы защиты информации	4		8	12
1.4	Технические средства добывания и инженерно-технической защиты информации	6		12	18
1.5	Организационные основы инженерно-технической защиты информации	4		8	12
1.6	Методическое обеспечение инженерно-технической защиты информации	4		8	12
3.1	Системы контроля и управления доступом (СКУД)	6	48	12	66
	Итого:	32	48	64	144

14. Методические указания для обучающихся по освоению дисциплины

1) При изучении дисциплины рекомендуется использовать следующие средства:

- рекомендуемую основную и дополнительную литературу;
- методические указания и пособия;
- контрольные задания для закрепления теоретического материала;
- электронные версии учебников и методических указаний для выполнения практических работ (при необходимости материалы рассылаются по электронной почте).

2) Для максимального усвоения дисциплины рекомендуется проведение письменного опроса (тестирование, решение задач) студентов по материалам лекций и практических работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала. Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.

3) При проведении практических занятий обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная проверка знаний основ информационной безопасности.

4) При переходе на дистанционный режим обучения для создания электронных курсов, чтения лекций он-лайн и проведения лабораторно-практических занятий используется информационные ресурсы Образовательного портала "Электронный университет ВГУ

(https:\\edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете.

5) При использовании дистанционных образовательных технологий и электронного обучения обучающиеся должны выполнять все указания преподавателей, вовремя подключаться к онлайн - занятиям, ответственно подходить к заданиям для самостоятельной работы.

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

(список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)

а) основная литература:

№ п/п	Источник
1	Сычев Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю. Н. Сычев; Российский экономический университет им. Г.В. Плеханова. - 1. - Москва : ООО "Научно-издательский центр ИНФРА-М", 2023. - 201 с. https://znanium.com/catalog/document?id=420080
2	Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс] : учебник для вузов / О. В. Прохорова. - 5-е изд., стер. - Санкт-Петербург : Лань, 2023. - 124 с. https://e.lanbook.com/book/293009
3	Игнатьев Е. Б. Защита информации: криптоалгоритмы хеширования [Электронный ресурс] : учебное пособие для вузов / Е. Б. Игнатьев. - Санкт-Петербург : Лань, 2023. - 264 с. https://e.lanbook.com/book/311792

б) дополнительная литература:

№ п/п	Источник
4	Креопалов В.В. Технические средства и методы защиты информации [Электронный ресурс]: учебное пособие/ В.В. Креопалов.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2011.— 278 c. http://www.iprbookshop.ru/10871.html
	Титов, А.А. Инженерно-техническая защита информации: учебное пособие / А.А. Титов. - Томск: Томский государственный университет систем управления и радиоэлектроники, 2010. - 195 с.; [Электронный ресурс]. -http://biblioclub.ru/index.php?page=book&id=208567
	Закон Российской Федерации « Об информации, информатизации и защите информации». [Электронный ресурс]. http://www.consultant.ru/document/cons_doc_LAW_61798/
	Иванов А.В. Защита речевой информации от утечки по акустоэлектрическим каналам [Электронный ресурс]: учебное пособие/ А.В. Иванов, В.А Трушин.— Электрон. текстовые данные.— Новосибирск: Новосибирский государственный технический университет, 2012.— 43 c. http://www.iprbookshop.ru/44919.html

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

№ п/п	Ресурс
8	«Университетская библиотека online» - Контракт № 3010-06/05-20 от 28.12.2020, «Консультант студента» - Контракт № 3010-06/06-20 от 28.12.2020, ЭБС «Лань» - Договор №3010-06/03-21 от 10.03.2021, *«РУКОНТ» (ИТС Контекстум) - Договор ДС-208 от 01.02.2018 ЭБС «Юрайт» - Договор № ДС-208 от 01.02.2021*
9	*Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).*
10	*Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/)*

16. Перечень учебно-методического обеспечения для самостоятельной работы

(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)

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.

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, указания по подготовке к зачету. 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):

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:

(при использовании лабораторного оборудования указывать полный перечень, при большом количестве оборудования можно вынести данный раздел в приложение к рабочей программе)

Учебная аудитория для проведения лекций: компьютер преподавателя, компьютер учащегося, мультимедиа оборудование (проектор, средства звуковоспроизведения), доска маркерная, специализированная мебель.

Аудитория для самостоятельной работы: учебная мебель, компьютер с возможностью подключения к сети «Интернет» и электронной платформе Электронного университета ВГУ необходимы компьютерные классы, помещения, оснащенные компьютерами с доступом к сети Интернет.

Компьютерный класс **Программное обеспечение (см.файл МТО):** Windows 10 (лицензионное ПО); Intellij IDEA Community Edition (свободное и/или бесплатное ПО); Paskal ABC NET (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); LibreOffice (свободное и/или бесплатное ПО); NetBeans IDE (свободное и/или бесплатное ПО); Adobe Reader (свободное и/или бесплатное ПО); Microsoft Visual Studio Community Edition (свободное и/или бесплатное ПО); Notepad ++ (свободное и/или бесплатное ПО); Free Pascal (свободное и/или бесплатное ПО); Anylogic (свободное и/или бесплатное ПО); Справочно-правовая система Гарант (лицензионное ПО); Mozilla Firefox (свободное и/или бесплатное ПО); 1С:Предприятие 8.3 (лицензионное ПО); Matlab (лицензионное ПО); 7-zip (свободное и/или бесплатное ПО (один из №1-4 корп. 1а, ауд. № 291, 293, 295, 387, 381), ПК-Intel-Core2/i3 14 шт., специализированная мебель: доска маркерная 1 шт., столы 14 шт., стулья 28 шт.; доступ к фондам учебно-методической документации и электронным изданиям, доступ к электронным библиотечным системам, выход в Интернет.

Типовой комплект учебного оборудования «Системы контроля и управления доступом»

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 (моду-ля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1.	Концепция инженерно-технической защиты информации	ПК-1	ПК-1.3	КИМы для проведения промежуточной аттестации Задания для контрольных работ Задания для лабораторных работ
2.	Теоретические основы инженерно-технической защиты информации	ПК-1	ПК-1.3	
3.	Физические основы защиты информации	ПК-1	ПК-1.3	
	Технические средства добывания и инженерно-технической защиты информации	ПК-2	ПК-2.2 ПК-2.3	
	Организационные основы инженерно-технической защиты информации	ПК-3	ПК-3.4 ПК-3.6	
	Методическое обеспечение инженерно-технической защиты информации	ПК-3	ПК-3.4 ПК-3.6	
Промежуточная аттестация форма контроля – зачет с оценкой				КИМы для проведения аттестации

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. Промежуточная аттестация

Контроль успеваемости по дисциплине осуществляется с помощью письменной работы на проверку знаний по разделам дисциплины (модулям).

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей аттестаций. На аттестации используется контрольно-измерительный материал, включающий в себя два-три вопроса.

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 (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, практические работы). При оценивании используется количественная шкала.

Критерии оценивания приведены таблице.

Критерии оценивания компетенций и шкала оценок

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие зна ний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач .	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольноизмерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	Неудовлетворительно

Контроль успеваемости по дисциплине осуществляется с помощью контрольной работы на проверку знаний по дисциплине и собеседования по ее результатам.

Для оценивания результатов обучения на зачете с оценкой используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

1) знание теоретических основ учебного материала, основных определений, понятий и используемой терминологии;

2) умение проводить обоснование и представление основных теоретических и практических результатов (теорем, алгоритмов, методик) с использованием математических выкладок, блок-схем, структурных схем и стандартных описаний к ним;

3) умение связывать теорию с практикой, иллюстрировать ответ примерами, в том числе, собственными, умение выявлять и анализировать основные закономерности, полученные, в том числе, в ходе выполнения лабораторно-практических заданий;

4) умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу;

5) владение навыками программирования и экспериментирования с компьютерными моделями алгоритмов обработки информации в рамках выполняемых практических заданий;

6) владение навыками проведения компьютерного эксперимента, тестирования компьютерных моделей алгоритмов обработки информации.

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций):

- высокий (углубленный) уровень сформированности компетенций;
- повышенный (продвинутый) уровень сформированности компетенций;
- пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на зачете с оценкой используется 4балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

В ходе промежуточной аттестации используется контрольно-измерительный материал, включающий в себя два-три вопроса.

Соотношение показателей, критериев и шкалы оценивания результатов обучения на зачете с оценкой представлено в следующей таблице.

Критерии оценивания компетенций и шкала оценок

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности,	Базовый уровень	Хорошо

испытывает затруднения при решении практических задач.		
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольноизмерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки	–	Неудовлетворительно

20.2 Итоговый контроль успеваемости

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

Вопросы:

1. Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации.
2. Принципы защиты информации техническими средствами.
3. Основные направления инженерно-технической защиты информации.
4. Показатели эффективности инженерно-технической защиты информации.
5. Понятие об информации как предмете защиты. Основные свойства информации как предмета защиты.
6. Семантическая информация, циркулирующая в человеческом обществе. Профессиональные языки.
7. Признаковая информация. Информация о видовых признаках, о признаках сигналов, о признаках веществ.
8. Структурирование информации.
9. Классификация демаскирующих признаков.
10. Опознавательные признаки и признаки деятельности.
11. Видовые демаскирующие признаки.
12. Демаскирующие признаки сигналов.
13. Демаскирующие признаки веществ. Именные, прямые и косвенные демаскирующие признаки.
14. Виды источников и носителей информации.
15. Прямые и косвенные источники семантической информации.
16. Принципы записи и съема информации с её носителя.
17. Источники функциональных сигналов. Понятие модуляции, манипуляции, демодуляции.
18. Побочные электромагнитные излучения и наводки Угрозы утечки информации. Угрозы преднамеренных воздействий. Угрозы случайных воздействий.
19. Технические каналы утечки информации: наблюдение, подслушивание, перехват.
20. Источники угроз безопасности информации.
21. Опасные сигналы и их источники.
22. Способы и средства наблюдения в оптическом диапазоне. Обработка информации в оптическом приемнике.

23. Способы и средства наблюдения в радиодиапазоне. Способы и средства перехвата сигналов.
24. Обработка информации в радиоприемнике.
25. Способы и средства подслушивания. Обработка информации в акустическом приемнике.
26. Типовая структура и виды технических каналов утечки информации.
27. Каналы утечки речевой информации.
28. Каналы утечки информации при её передаче по каналам связи.
29. Каналы утечки видовой информации.
30. Акустические и виброакустические каналы утечки речевой информации из объемов выделенных помещений.
31. Каналы утечки информации за счет побочных электромагнитных излучений и наводок.
32. Средства маскировки и дезинформирования в оптическом и радиодиапазонах.
33. Средства звукоизоляции из звукопоглощения.
34. Средства обнаружения, локализации и подавления сигналов закладных устройств.
35. Средства подавления сигналов акустоэлектрических преобразователей, фильтрации и заземления.
36. Генераторы линейного и пространственного зашумления.

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

ПК-1 Способен проводить анализ требований и выполнять работы по проектированию программных и аппаратных компонент системы безопасности компьютерных систем и сетей, в том числе с использованием современных методов и средств защиты информации

1. Замысел защиты информации:

а) основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации;

б) деятельность по обеспечению защиты не криптографическими методами информации от ее утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию;

в) совокупность объекта защиты, физической среды и средства технической разведки, которым добывается защищаемая информация.

2. Какие законы существуют в России в области компьютерного права?

1) О государственной тайне
2) об авторском праве и смежных правах
3) о гражданском долге
4) о правовой охране программ для ЭВМ и БД
5) о правовой ответственности
6) об информации, информатизации, защищенности информации

3. Какие существуют основные уровни обеспечения защиты информации?

1) законодательный
2) административный

3) программно-технический

4) физический

5) вероятностный

6) процедурный

7) распределительный

4. Физические средства защиты информации

1) средства, которые реализуются в виде автономных устройств и систем

2) устройства, встраиваемые непосредственно в аппаратуру, АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу

3) это программы, предназначенные для выполнения функций, связанных с защитой информации

4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств

5. Технические средства защиты информации

1) средства, которые реализуются в виде автономных устройств и систем

2) устройства, встраиваемые непосредственно в аппаратуру, АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу

3) это программы, предназначенные для выполнения функций, связанных с защитой информации

4) средства, которые реализуются в виде электрических, электромеханических и электронных устройств

6. К аспектам ИБ относятся

1) дискретность

2) целостность

3) конфиденциальность

4) актуальность

5) доступность

7. Выделите группы, на которые делятся средства защиты информации:

1) физические, аппаратные, программные, криптографические, комбинированные;

2) химические, аппаратные, программные, криптографические, комбинированные;

3) физические, аппаратные, программные, этнографические, комбинированные;

8. Надежным средством отвода наведенных сигналов на землю служит

Запишите ответ: _____

Верный ответ: "**заземление**".

ПК-2 Способен принимать участие в экспертизе и анализе уязвимостей, угроз и инцидентов информационной безопасности в компьютерных системах и сетях

1. Организационные угрозы подразделяются на (Выберите несколько из 4 вариантов ответа):

1) угрозы воздействия на персонал

2) физические угрозы

3) действия персонала

4) несанкционированный доступ

2. Виды технической разведки (по месту размещения аппаратуры) (Выберите несколько из 7 вариантов ответа):

1) космическая

2) оптическая

3) наземная

4) фотографическая

5) морская

6) воздушная

7) магнитометрическая

3. Основные группы технических средств ведения разведки (Выберите несколько из 5 вариантов ответа):

1) радиомикрофоны

2) фотоаппараты

3) электронные "уши"

4) дистанционное прослушивание разговоров

5) системы определения местоположения контролируемого объекта

4. Разновидности угроз безопасности (Выберите несколько из 6 вариантов ответа):

1) техническая разведка

2) программные

3) программно-математические

4) организационные

5) технические

6) физические

5. Потенциально возможное событие, действие, процесс или явление, которое может

причинить ущерб чьих-нибудь данных, называется (Выберите один из 4 вариантов ответа):

1) угрозой;

2) опасностью;

3) намерением;

4) предостережением.

6. Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется (Выберите один из 4 вариантов ответа):

1) системой угроз;

2) системой защиты;

3) системой безопасности;

4) системой уничтожения.

7. Выделите группы, на которые делятся средства защиты информации (Выберите один из 3 вариантов ответа):

1) физические, аппаратные, программные, криптографические, комбинированные;

2) химические, аппаратные, программные, криптографические, комбинированные;

3) физические, аппаратные, программные, этнографические, комбинированные;

8. Укажите соответствие для всех 4 вариантов ответа:

1) это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок	– защита информации от утечки по акустическому каналу – Защита информации от утечки по визуально-оптическому каналу – Защита информации от утечки по электромагнитным каналам

2) это комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны в виде производственных или промышленных отходов	– Защита информации от утечки по материально-вещественному каналу
3) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей	
4) это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии	
3; 4; 1; 2;	

1. Средства защиты информации:

а) должны проходить контроль на отсутствие недекларированных возможностей;

б) не должны проходить контроль на отсутствие недекларированных возможностей;

в) должны проходить контроль на отсутствие недекларированных возможностей по усмотрению оператора.

2. Системное программное обеспечение:

а) проходит контроль на отсутствие недекларированных возможностей;

б) не проходит контроль на отсутствие недекларированных возможностей;

в) проходит контроль на отсутствие недекларированных возможностей по усмотрению оператора.

3. Прикладное программное обеспечение:

а) проходит контроль на отсутствие недекларированных возможностей;

б) не проходит контроль на отсутствие недекларированных возможностей;

в) проходит контроль на отсутствие недекларированных возможностей по усмотрению оператора.

4. Аттестацию информационных систем по требованиям безопасности информации:

а) оператор проводит самостоятельно, с привлечением штатных специалистов по защите информации;

б) проводит орган по аттестации, аккредитованный ФСТЭК России;

в) государственные информационные системы не подлежат аттестации.

5. Что относится к основным механизмам защиты компьютерной системы от несанкционированного доступа:

а) физическая защита компонент компьютерной системы, идентификация и аутентификация, разграничение доступа, контроль обращений к защищаемой информации;

б) дублирование информации, создание отказоустойчивых компьютерных систем, блокировка ошибочных операций, повышение надежности компьютерных систем;

в) сегментация сетей с помощью коммутаторов и межсетевых экранов, шифрование информации.

6. Какие основные способы разграничения доступа применяются в компьютерных системах:

а) дискреционный и мандатный;

б) по специальным спискам и многоуровневый;

в) по группам пользователей и специальным разовым разрешениям.

7. Кто должен анализировать журнал аудита безопасности компьютерной системы:

а) администратор;

б) аудитор;

в) начальник.

8. Аутентификация это:

а) процесс предъявления пользователем идентификатора;

б) процесс подтверждения подлинности;

в) регистрация всех обращений к защищаемой информации.

9. Какие основные компоненты входят в состав удостоверяющего центра:

а) центр сертификации, центр авторизации, АРМ администратора; б) центр регистрации, центр авторизации, АРМ администратора;

в) центр сертификации, центр регистрации, АРМ администратора.

10. Что собой представляет сертификат электронного ключа подписи:

а) это электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП;

б) это документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки ЭП владельцу сертификата ключа проверки ЭП;

в) это логическая посимвольная свертка подписываемого сообщения, зашифрованная на открытом ключе получателя.

11. Перечислите основные компоненты программного комплекса ViPNet CUSTOM:

а) client, administrator, coordinator;

б) client, administrator, certificate center;

в) administrator, coordinator, certificate center.

ПК-3 Способен участвовать в работах по проектированию систем защиты информации в компьютерных системах и сетях при решении профессиональных, исследовательских и прикладных задач

a) Длинной пароля
b) Частотой смены пароля
c) Историей пароля
d) Содержимым пароля
e) Все из перечисленного
f) Ничего из перечисленного

2) Физическая безопасность обеспечивает защиту информационных систем

a) Защиту от пожара
b) Защиту от вирусов
c) Защиту от сбоев
d) Защиту от кражи

3) 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

4) 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.

5) 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.

6. Какой нормативный документ является приоритетным в РФ

А) Федеральные законы РФ

Б) Международные акты

В) Постановления Правительства РФ

Г) Указы президента РФ

7. 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.**

1. Какие параметры электрических цепей чаще всего изменяются под воздействием

акустической волны в пассивных акустоэлектрических преобразователях?

- **емкость;**
- длина.
- сопротивление.

2. Какой показатель используется для оценки защищенности речевой информации?

- громкость;
- **разборчивость;**
- спектр.

3. Кто является основным ответственным за определение уровня классификации

информации?

- пользователь;
- **владелец;**
- руководитель предприятия.

4. Что предписано сделать с персональными данными после достижения целей, с

которыми они обрабатывались?

- обезличить;
- хранить;
- **уничтожить.**

5. Как называются закладки, использующие для передачи информации силовые линии?

- радиозакладки;
- **сетевые закладки;**
- стетоскопы.

6. К каналам утечки информации относят:

- разглашение;
- отказ средств обработки;
- **несанкционированный доступ.**

7. Укажите правильный ключ реестра, отключающего автозапуск с компакт диска

- **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Cdrom, Autorun = 0**
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dvdrom**,** Autorun = 0
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\BlueRayDisc, Autorun = 0

8. Укажите правильный ключ реестра,отключающий автозапуск со всех носителей

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\ Explorer,
- NoDriveTypeAutoRun = 0
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\ Explorer,
- NoDriveTypeAutoRun = 1
- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer,**
- **NoDriveTypeAutoRun = FF**

9. Укажите правильный ключ реестра, переключающий управление автозапуском на INI файл DoesNotExist

- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\IniFileMapping\Auto**
- **run.inf = @SYS:DoesNotExist**
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\IniFileMapping\Autorun.in
- f = USE %DoesNotExist%
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\IniFileMapping\Autorun.in
- f = USE %DoesNotExist.INI%

10. Разговорный тракт устраняет:

- шумы;
- искажения;
- **местный эффект**

11. Стандарт GSM использует уплотнение каналов:

- **частотное;**
- **временное;**
- кодовое.

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