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

УТВЕРЖДАЮ

Заведующий кафедрой
функционального анализа
и операторных уравнений

Каменский М.И.
25.05.23г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.29 Информационная безопасность

1. Код и наименование специальности: 01.05.01 фундаментальные математика и механика

2. Специализация: Современные методы теории функций в математике и механике

3. Квалификация выпускника: Математик. Механик. Преподаватель

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: функционального анализа и операторных уравнений

6. Составители программы: Сидельникова Софья Юрьевна, преподаватель; математический факультет, кафедра функционального анализа и операторных уравнений

7. Рекомендована: НМС математического факультета, протокол № 0500-06 от 25.05.2023г.

8. Учебный год: 2026–2027 **Семестр:** 7

9. **Цели и задачи учебной дисциплины:**

Цели освоения учебной дисциплины:

- изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

Задачи учебной дисциплины:

- изучение характеристик основных угроз информационной безопасности, каналов утечки информации и методов компьютерного шпионажа;
- получение представлений о существующих правовых, организационных методах и технических средствах защиты информации от несанкционированного доступа и от модификации и удаления;
- освоение критериев эффективности мер по защите информации.

10. Место учебной дисциплины в структуре ООП: дисциплина относится к обязательной части блока 1.Дисциплины(модули). Для изучения и освоения дисциплины нужны знания из предшествующих курсов: Теория графов и математическая логика, Теория вероятностей, математическая статистика и теория случайных процессов, Алгоритмы дискретной математики, Операционные системы и сети, Программные аппаратные средства информатики, Программирование для ЭВМ.

Знания и умения, приобретенные студентами в результате изучения дисциплины, будут использоваться при выполнении курсовых и дипломных работ, связанных с математическим моделированием в области информационной безопасности и обработкой наборов данных, а также при прохождении производственной практики.

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
ОПК-3	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-3.1	Осуществляет поиск, сбор, хранение, обработку, представление информации при решении задач профессиональной деятельности.	Знать: - принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности. Уметь: - осуществлять поиск, сбор, хранение, обработку, представление информации при решении задач профессиональной деятельности. Владеть навыками: - подбора и использования информационных технологйи при решении задач профессиональной деятельности.
		ОПК-3.2	Подбирает и использует информационные технологии при решении задач профессиональной деятельности	
ОПК-2	Способен создавать, анализировать и реализовывать новые математические модели в современном естествознании, технике, экономике и управлении	ОПК-2.1	Владеет основами планирования экспериментов с математическими моделями, знает численные и численно-аналитические методы построения решений.	Знать: - новые математические модели в современном естествознании, технике, экономике и управлении. Уметь: - выбирать методы моделирования и анализировать моделируемую систему. Владеть: - основами планирования экспериментов с математическими моделями, знает числен-
		ОПК-	Умеет выбирать	

		2.2	методы моделирования и анализировать моделируемую систему.	ные и численно-аналитические методы построения решений.
		ОПК-2.3	Имеет практический опыт разработки математических моделей и их численной реализации	
ОПК-5	Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения	ОПК-5.1	Использует основные принципы алгоритмизации задач в рамках профессиональной деятельности и разработки компьютерных программ.	Знать: - алгоритмы и компьютерные программы, пригодные для практического применения. Уметь: - использовать основные принципы алгоритмизации задач в рамках профессиональной деятельности и разработки компьютерных программ. Владеть навыками: - тестирования и отладки компьютерных программ с целью апробации разработанных моделей и алгоритмов.
		ОПК-5.2	Проводит тестирование и отладку компьютерных программ с целью апробации разработанных моделей и алгоритмов.	

12. Объем дисциплины в зачетных единицах/час — 3/108

Форма промежуточной аттестации: зачет

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость	
		Всего	По семестрам
			7-й семестр
Аудиторные занятия		68	68
в том числе:	лекции	34	34
	практические	34	34
	лабораторные		
Самостоятельная работа		40	40
в том числе: курсовая работа(проект)			
Форма промежуточной аттестации *(экзамен – 36 час.)*			
Итого:		108	108

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1. Лекции		
1	Введение в теорию информационной безопасности	Основные понятия и определения. Концептуальные основы информационной безопасности и защиты информации. Обзор цифровых технологий, и их связь со сферой информационной безопасности.
2	Структура информационных	Понятие об информационных ресурсах. Понятия интеллек-

	ресурсов. Интеллектуальная собственность и коммерческая тайна.	туальной собственности и коммерческой тайны, их структура. Персональные данные. Принципы информационной безопасности.
3	Угрозы информационной безопасности и их классификация.	Угрозы информационным ресурсам: угрозы несанкционированного доступа, модификации и удаления информации; угрозы криминогенного характера, природного и техногенного характера, угрозы, связанные с неквалифицированным пользованием информационными ресурсами. Компьютерный шпионаж, его цели и методы. Внутренние и внешние факторы, способствующие компьютерному шпионажу. Характеристика каналов утечки информации. Активный и пассивный доступ к информационным ресурсам.
4	Правовые аспекты защиты информации.	Понятие о правовых средствах защиты информации. Законы, регулирующие деятельность по защите информации. Охрана объектов интеллектуальной собственности. Проблемы, возникающие при реализации правовых мер защиты информации
5	Организационные мероприятия, направленные на защиту информации.	Ограничение и разграничение доступа к информации. Дублирование важной информации на разнотипных носителях. Многоуровневая система защиты информации.
6	Программно-аппаратные средства защиты информации	Пароли и системы с многоуровневым доступом. «Защита от дурака» в компьютерных программах. Защита программ и электронных баз данных. Антивирусные программы. Защита каналов связи. Повреждение информации в каналах связи и средства борьбы с ним.
7	Математические методы и модели в задачах защиты информации.	Методы сжатия информации. Криптографические методы защиты информации. Шифрование с симметричными и ассиметричными ключами.
8	Эффективность мероприятий по защите информации	Частный функциональный критерий информационной безопасности и его формула для мероприятий по предотвращению несанкционированного доступа. Структура понесенного и предотвращенного ущерба от несанкционированного доступа к информации. Структура затрат на защиту информации.
2. Лабораторные занятия		
1	Введение в теорию информационной безопасности	Основные понятия и определения. Концептуальные основы информационной безопасности и защиты информации
2	Структура информационных ресурсов. Интеллектуальная собственность и коммерческая тайна.	Понятие об информационных ресурсах. Понятия интеллектуальной собственности и коммерческой тайны, их структура. Персональные данные. Принципы информационной безопасности.
3	Угрозы информационной безопасности и их классификация.	Угрозы информационным ресурсам: угрозы несанкционированного доступа, модификации и удаления информации; угрозы криминогенного характера, природного и техногенного характера, угрозы, связанные с неквалифицированным пользованием информационными ресурсами. Компьютерный шпионаж, его цели и методы. Внутренние и внешние факторы, способствующие компьютерному шпионажу. Характеристика каналов утечки информации. Активный и пассивный доступ к информационным ресурсам.
4	Правовые аспекты защиты информации.	Понятие о правовых средствах защиты информации. Законы, регулирующие деятельность по защите информации. Охрана объектов интеллектуальной собственности. Проблемы, возникающие при реализации правовых мер защиты информации
5	Организационные мероприятия, направленные на защиту информации.	Ограничение и разграничение доступа к информации. Дублирование важной информации на разнотипных носителях. Многоуровневая система защиты информации.
6	Программно-аппаратные средства защиты информации	Пароли и системы с многоуровневым доступом. «Защита от дурака» в компьютерных программах. Защита программ и электронных баз данных. Антивирусные программы. Защита каналов связи. Повреждение информации в каналах связи и

		средства борьбы с ним.
7	Математические методы и модели в задачах защиты информации.	Методы сжатия информации. Криптографические методы защиты информации. Шифрование с симметричными и ассиметричными ключами.
8	Эффективность мероприятий по защите информации	Частный функциональный критерий информационной безопасности и его формула для мероприятий по предотвращению несанкционированного доступа. Структура понесенного и предотвращенного ущерба от несанкционированного доступа к информации. Структура затрат на защиту информации.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные	Самостоятельная работа	Всего
1	Введение в теорию информационной безопасности	2	2	4	8
2	Структура информационных ресурсов. Интеллектуальная собственность и коммерческая тайна.	2	2	4	8
3	Угрозы информационной безопасности и их классификация.	2	2	4	8
4	Правовые аспекты защиты информации.	2	2	4	8
5	Организационные мероприятия, направленные на защиту информации.	2	2	4	8
6	Программно-аппаратные средства защиты информации	3	2	5	10
7	Математические методы и модели в задачах защиты информации.	3	4	5	12
8	Эффективность мероприятий по защите информации	2	2	4	8
	Итого	34	34	40	108

14. Методические указания для обучающихся по освоению дисциплины

Преподавание дисциплины заключается в чтении лекций и проведении лабораторных занятий. На лекциях рассказывается теоретический материал, на лабораторных занятиях решаются примеры по теоретическому материалу, прочитанному на лекциях. При изучении курса «Информационная безопасность» обучающимся следует внимательно слушать и конспектировать материал, излагаемый на аудиторных занятиях. Для его понимания и качественного усвоения обучающимся рекомендуется следующая последовательность действий.

1. После каждой лекции студентам рекомендуется подробно разобрать прочитанный теоретический материал, выучить все определения, разобрать примеры, решенные на лекции. Перед следующей лекцией обязательно повторить материал предыдущей лекции.
2. Перед лабораторным занятием обязательно повторить лекционный материал. После лабораторного занятия еще раз разобрать решенные на этом занятии примеры, после приступить к выполнению домашнего задания. Если при решении примеров, заданных на дом, возникают вопросы, обязательно задать на следующем лабораторном занятии или в присутствующий час преподавателю.
3. При подготовке к лабораторным занятиям повторить основные понятия по темам, изучить примеры. Решая задачи, предварительно понять, какой теоретический мате-

риал нужно использовать. Наметить план решения, попробовать на его основе решить лабораторные задачи.

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

а) основная литература:

№ п/п	Источник
1	*Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2019. — 324 с. — Режим доступа://e.lanbook.com/book/114688*
2	*Ярочкин, В. И. Информационная безопасность : учебник / В. И. Ярочкин. — 5-е изд. — Москва : Академический Проект, 2020. — 544 с. — ISBN 978-5-8291-3031-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/132242*

б) дополнительная литература:

№ п/п	Источник
3	*Фот, Ю. Д. Стандарты информационной безопасности : учебное пособие / Ю. Д. Фот. — Оренбург : ОГУ, 2018. — 226 с. — ISBN 978-5-7410-2297-9. — Текст : электронный // Лань : 6электронно-библиотечная система. — URL: https://e.lanbook.com/book/159804*
4	*Давидюк, Н. В. Мониторинг безопасности информационных систем : учебное пособие / Н. В. Давидюк, И. М. Космачева. — Санкт-Петербург : Интермедия, 2020. — 116 с. — ISBN 978-5-4383-0204-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/161352*
5	*Бирюков, А. А. Информационная безопасность: защита и нападение / А. А. Бирюков. — 2-е изд. — Москва : ДМК Пресс, 2017. — 434 с. — ISBN 978-5-97060-435-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/93278*
6	*Филиппов, Б.И. Информационная безопасность. Основы надежности средств связи : учебник / Б.И. Филиппов, О.Г. Шерстнева. – Москва ; Берлин : Директ-Медиа, 2019. – 241 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=499170*
7	*Баранова, Елена Константиновна. Информационная безопасность и защита информации : учебное пособие : [для студ., обучающихся по направлению "Прикладная информатика"] / Е.К. Баранова, А.В. Бабаш .— 4-е изд. перераб. и доп. — Москва : РИОР : ИНФРА-М, 2019 .— 334, [1] с. : ил., табл. — (Высшее образование) .— Библиогр.: с. 327-330.*

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

№ п/п	Источник
9	*Электронно-библиотечная система «Лань». - Режим доступа: https://e.lanbook.com*
10	*Электронный каталог Научной библиотеки Воронежского государственного университета. – Режим доступа: http//:www.lib.vsu.ru.*

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1.	Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2019. — 324 с. — Режим доступа://e.lanbook.com/book/114688
2.	Ярочкин, В. И. Информационная безопасность : учебник / В. И. Ярочкин. — 5-е изд. — Москва : Академический Проект, 2020. — 544 с. — ISBN 978-5-8291-3031-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/132242
3.	*Фот, Ю. Д. Стандарты информационной безопасности : учебное пособие / Ю. Д. Фот. — Оренбург : ОГУ, 2018. — 226 с. — ISBN 978-5-7410-2297-9. — Текст : электронный // Лань :* 6электронно-библиотечная система. — URL: https://e.lanbook.com/book/159804

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

При реализации учебной дисциплины, могут использоваться дистанционные образовательные технологии (курс на сайте edu.vsu.ru на платформе Moodle). При проведении занятий в дистанционном режиме обучения используются информационные и технические ресурсы Образовательного портала «Электронный университет ВГУ»

Зональная научная библиотека, электронный каталог Научной библиотеки (http://www.lib.vsu.ru)

18. Материально-техническое обеспечение дисциплины:

Учебная аудитория: специализированная мебель

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	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Введение в теорию информационной безопасности	ОПК-2, ОПК-3, ОПК-5	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-5.1, ОПК-5.2	Домашнее задание, контрольная работа
2	Структура информационных ресурсов. Интеллектуальная собственность и коммерческая тайна.	ОПК-2, ОПК-3, ОПК-5	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-5.1, ОПК-5.2	Домашнее задание, контрольная работа
3	Угрозы информационной безопасности и их классификация.	ОПК-2, ОПК-3, ОПК-5	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-5.1, ОПК-5.2	Домашнее задание, контрольная работа
4	Правовые аспекты защиты информации.	ОПК-2, ОПК-3, ОПК-5	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-5.1, ОПК-5.2	Домашнее задание, контрольная работа
5	Организационные мероприятия, направленные на защиту информации.	ОПК-2, ОПК-3, ОПК-5	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-5.1, ОПК-5.2	Домашнее задание, контрольная работа
6	Программно-аппаратные средства защиты информации	ОПК-2, ОПК-3, ОПК-5	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-5.1, ОПК-5.2	Домашнее задание, контрольная работа
7	Математические методы и модели в задачах защиты информации.	ОПК-2, ОПК-3, ОПК-5	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-5.1, ОПК-5.2	Домашнее задание, контрольная работа
8	Эффективность мероприятий по защите информации	ОПК-2, ОПК-3, ОПК-5	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-3.1, ОПК-3.2, ОПК-5.1, ОПК-5.2	Домашнее задание, контрольная работа
	Промежуточная аттестация форма контроля – зачёт			КИМ(зачет)

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Текущая аттестация проводится в форме лабораторных работ, докладов и контрольной работы.

20.1.1. Лабораторные работы:

Лабораторные работы проводятся по различным методам шифрования. Примеры:

Лабораторная работа №1

Криптографические методы защиты информации.
Шифрование методом простой замены.

Цель работы: Зашифровать текст методом простой замены.
Задание:

1) Взять текст, примерно 2500 символов.
2) Привести этот текст к форме, удобной для шифрования:

- Убрать все знаки препинания.
- Перевести весь текст в верхний регистр.
- Объединить «парные» буквы, такие как (е, ё), (и, й), (ъ, ь).

После преобразований в тексте должно остаться не менее 2000 символов.

3) Выбрать ключ для шифрования методом простой замены.

*При этом **не использовать** слабые ключи. **Не использовать** метод Цезаря, Атбаш и т.д.*

4) Посчитать статистику для каждой буквы. Индекс совпадения.
5) Написать программу для шифрования текста методом простой замены.

Лабораторная работа №2

Шифр Виженера.

Задание:

1. Взять текст, примерно 2500 символов, преобразовать его как в лабораторной работе №1
2. Выбрать ключ - одно слово.
3. Зашифровать его методом полиалфавитной замены(шифром Виженера).
4. Посчитать статистику для каждой буквы шифротекста, посчитать индекс совпадения.
5. Написать программу для шифрования текста методом простой замены.

20.1.2. Контрольные работы:

Пример контрольного задания (вариант задания):

Контрольная работа
по дисциплине «Информационная безопасность»
Вариант №___

В результате шифрования методом Вижинера был получен следующий шифртекст: «СПЦСЗЗЮУГИВЕБЬБТЖЩИОБ». Прочитайте этот шифртекст,

если известно, что шифрующая последовательность содержит только символы А, Б и В.

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

Собеседование по билетам к зачету:

1. Введение в теорию информационной безопасности
2. Структура информационных ресурсов. Интеллектуальная собственность и коммерческая тайна.
3. Угрозы информационной безопасности и их классификация.
4. Правовые аспекты защиты информации.
5. Организационные мероприятия, направленные на защиту информации.
6. Программно-аппаратные средства защиты информации
7. Математические методы и модели в задачах защиты информации.
8. Эффективность мероприятий по защите информации.

Пример КИМ

Контрольно-измерительный материал № ___

1. Угрозы информационной безопасности.

2. Методы и средства инженерной защиты объектов информатизации

Преподаватель _____ _____.
подпись расшифровка подписи

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

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

Текущая аттестация проводится в форме лабораторных работ и контрольной работы.

Промежуточная аттестация проводится в форме зачета и включает в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и практическое задание, позволяющее оценить степень сформированности умений и навыков.

При оценивании используется следующая шкала:

Зачтено ставится, если обучающийся демонстрирует полное или удовлетворительное соответствие знаний, умений, навыков приведенным в таблицах показателям, свободно или с незначительными ошибками оперирует приобретенными знаниями, умениями, применяет их при решении практических задач;

Не зачтено ставится, если обучающийся демонстрирует явное несоответствие знаний, умений, навыков приведенным в таблицах показателям.

Критерии оценивания компетенций	Уровень сформиро-	Шкала оценок

	ванности компетенций	
Обучающийся в полной мере владеет понятийным аппаратом в области программирования и технологии работы на ЭВМ, способен иллюстрировать ответ примерами, фактами, применять теоретические знания для решения практических задач программирования, СУБД и сетевых технологий.	*Повышенный уровень*	*Зачтено*
У обучающегося сформированы знания, умения и навыки программирования и технологии работы на ЭВМ; он способен иллюстрировать ответ примерами, фактами, применять теоретические знания для решения практических задач; но допускает отдельные несущественные пробелы в своих знаниях, допускает ошибки при выполнении практических задач.	*Базовый уровень*	
У обучающегося сформированы неполные знания, умения и навыки; он допускает отдельные существенные пробелы в своих знаниях, допускает существенные ошибки при выполнении практических задач.	*Пороговый уровень*	
Сформированы лишь фрагментарные знания, умения и навыки или знания, умения и навыки отсутствуют	*–*	*Не Зачтено*

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

1) закрытые задания (тестовые):

1. Что такое криптография?
   1. Раздел информатики, изучающий проблемы анализа, обработки и представления данных в цифровой форме
   2. Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов
   3. Процесс интеграции цифровых технологий во все аспекты бизнес-деятельности
   4. Наука о защите данных

   Ответ: 4

2. Симметричное шифрование – это шифрование, в котором для зашифрования и расшифрования используется
   1. 1 ключ
   2. 2 ключа
   3. 3 ключа
   4. 4 ключа

   Ответ: 1
   Решение: Симметричное шифрование предусматривает использование одного и того же ключа и для зашифрования, и для расшифрования.
3. Отметьте, что из перечисленного относится ко внешним угрозам информационной безопасности (множественный выбор):
   1. Утечки информации
   2. DDoS-атаки
   3. Неавторизованный доступ
   4. Фишинг

Ответ: 2,4
Решение: ко внешним угрозам относятся DDoS-атаки и фишинг.

4. Что не относится к сведениям конфиденциального характера?
   1. Персональные данные
   2. Сведения, составляющие тайну следствия
   3. Сведения о сущности изобретения
   4. защищаемые государством сведения в области его военной деятельности, распространение которых может нанести ущерб безопасности РФ.

   Ответ:4
   Решение: защищаемые государством сведения в области его военной деятельности, распространение которых может нанести ущерб безопасности РФ относятся к государственной тайне.

5. Кто имеет право выдавать сертификаты усиленной квалифицированной электронной подписи?
   1. Аккредитованный удостоверяющий центр
   2. Организация, имеющая лицензию на деятельность по технической защите конфиденциальной информации
   3. Любой удостоверяющий центр
   4. Организация, имеющая лицензию на деятельность по техническому обслуживанию, модернизации и распространению шифровальных средств

   Ответ: 1
   Решение: сертификаты усиленной квалифицированной электронной подписи имеет право выдавать только аккредитованный удостоверяющий центр.

2) открытые задания:

1. Напишите число возможных комбинаций имеет пароль из 3 символов, если пользователь использует только цифры.
   Ответ: 1000
   Решение: В данном случае речь идет о размещении с повторениями, так у нас 3 позиции в пароле, цифры могут повторяться. Число комбинаций для такого пароля равно $10^3 = 1000$
2. Вставьте пропущенное слово. Основными составляющими информационной безопасности являются конфиденциальность, […], доступность.

   Ответ: целостность
   Решение: Основными составляющими информационной безопасности являются конфиденциальность, целостность, доступность.
3. Вставьте пропущенное слово. […] информационной безопасности – это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

   Ответ: Угроза
   Решение: Угроза информационной безопасности – это совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

4. Напишите число возможных комбинаций имеет пароль из 3 символов, если пользователь использует 1 строчную букву латинского алфавита на первой позиции, а для двух других позиций пароля использует цифры.
   Ответ: 2600
   Решение: В данном случае используется правило умножения, так у нас 3 позиции в пароле, цифры могут повторяться, и одна буква зафиксирована на первой позиции пароля. Число комбинаций для такого пароля равно
   $26 * 10 * 10 = 2600$
5. Вредоносный код, обладающий способностью к распространению путем внедрения в другие программы – это…
   Ответ: вирус
   Решение: Вредоносный код, обладающий способностью к распространению путем внедрения в другие программы – это вирус.

Критерии и шкалы оценивания заданий ФОС:

1) Задания закрытого типа (выбор одного варианта ответа, верно/неверно):

- 1 балл – указан верный ответ;
- 0 баллов – указан неверный ответ.

2) Задания закрытого типа (множественный выбор):

- 2 балла – указаны все верные ответы;
- 0 баллов — указан хотя бы один неверный ответ.

3) Задания закрытого типа (на соответствие):

- 2 балла – все соответствия определены верно;
- 0 баллов – хотя бы одно сопоставление определено неверно.

4) Задания открытого типа (короткий текст):

- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ.

5) Задания открытого типа (число):

- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ.

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