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

УТВЕРЖДАЮ

Заведующий кафедрой
функционального анализа и операторных уравнений
наименование кафедры, отвечающей за реализацию дисциплины

Каменский М.И.
подпись, расшифровка подписи
25.05.2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.32 Информационная безопасность

1. Код и наименование направления подготовки: 01.03.01 математика

2. Профиль подготовки: дифференциальные уравнения, динамические системы и оптимальное управление

3. Квалификация выпускника: бакалавр
4. Форма обучения: очная

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

6. Составители программы: Завгородний Михаил Григорьевич**,** канд. физ-мат. наук, доцент
7. Рекомендована: научно-методическим советом математического факультета, протокол от 25.05.2023, № 0500-06
8. Учебный год:2026-2027 **Семестр(ы):** 8

9.Цели и задачи учебной дисциплины:

Цели изучения 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.Дисциплина(модули). Для изучения и освоения дисциплины нужны знания из предшествующих курсов: Дискретная математика, Теория вероятностей, Теория чисел, Технология программирования и работа на ЭВМ. Знания и умения, приобретенные студентами в результате изучения дисциплины, будут использоваться при выполнении курсовых и дипломных работ, связанных с математическим моделированием в области защиты информации.

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-4	Способен решать задачи профессиональной деятельности с использованием существующих информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-4.2	Проверяет выполнение требований защиты информации и применяет их при решении профессиональных задач	Знать: основные принципы обработки научных результатов Уметь: выявлять и оценивать направления угроз научной информации Владеть: навыками организации защиты научной информации
		ОПК-4.3	Применяет навыки информационно-коммуникационных технологий для создания и обработки информации	Знать: основные принципы работы систем управления базами данных и телекоммуникационных сетей с учетом требований информационной безопасности Уметь: применять требования информационной безопасности при работе с системами управления базами данных и телекоммуникационными сетями Владеть: навыками организации безопасной работы систем управления базами данных и телекоммуникационных сетей Владеть: навыками организации безопасной работы систем управления базами данных и телекоммуникационных сетей
ОПК-1	Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности	ОПК-1.1	Применяет базовые знания, полученные в области математических и(или) естественных наук	Знать: основные принципы проектирования и разработки системы информационной безопасности Уметь: выявлять и оценивать направления информационных угроз Владеть: навыками организации аппаратно-программной защиты информации
		ОПК-1.2	Оценивает и формулирует актуальные и значимые проблемы фундаментальной	Знать: основные проблемы защиты информации Уметь: применять методы фундаментальной математики для решения задач защиты информации Владеть: навыками математического

			математики	моделирования и программирования задач защиты информации
		ОПК-1.3	Анализирует и применяет навыки выбора методов решения задач профессиональной деятельности на основе теоретических знаний	Знать: основные методы решения задач профессиональной деятельности Уметь: выявлять и оценивать направления информационных угроз при решении задач профессиональной деятельности Владеть: навыками организации защиты информации при решении задач профессиональной деятельности
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: стандартные задачи профессиональной деятельности на основе информационной и библиографической структуры с применением информационно-коммуникационных технологий уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий владеть: навыками решения стандартных задач профессиональной деятельности на основе ин- формационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
		ОПК-5.2	Проводит тестирование и отладку компьютерных программ с целью апробации разработанных моделей и алгоритмов	Знать: основные компьютерные модели и алгоритмы. Уметь: проводить тестирование и отладку компьютерных программ Владеть: механизмом создания программного продукта при выполнении конкретных задач в изучаемой области.

12. Объем дисциплины в зачетных единицах/час.(*в соответствии с учебным планом)* **— 2/72.**

Форма промежуточной аттестации*(зачет/экзамен)* *зачет.*

13. Виды учебной работы

Вид учебной работы		Трудоемкость	
		Всего	По семестрам
			8 семестр
Аудиторные занятия		24	24
в том числе:	лекции	12	12
	практические		
	лабораторные	12	12
Самостоятельная работа		48	48
в том числе: курсовая работа		-	-

(проект)		
Форма промежуточной аттестации *(зачет – __час.)*		зачет
Итого:	72	72

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
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 ассимметричными 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	1	1	4	6
2	Структура информационных ресурсов. Интеллектуальная собственность и коммерческая	1	1	4	6

	тайна.				
3	Угрозы информационной безопасности и их классификация.	1	1	6	8
4	Правовые аспекты защиты информации.	1	2	6	9
5	Организационные мероприятия, направленные на защиту информации.	2	2	6	10
6	Программно-аппаратные средства защиты информации	1	1	6	8
7	Математические методы и модели в задачах защиты информации.	4	3	10	17
8	Эффективность мероприятий по защите информации	1	1	6	8
	Итого	12	12	48	72

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

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)*

№ п/п	Источник
1	*Мельников, Владимир Павлович. Информационная безопасность и защита информации : учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова .— М. : ACADEMIA, 2006 .— 330 с. : ил .— (Высшее профессиональное образование. Информатика и вычислительная техника) .— Библиогр.: с.327-328 .— ISBN 5-7695-2592-4.*
2	*Чубукова, Светлана Георгиевна. Основы правовой информатики (юридические и математические вопросы информатики) : учебное пособие для студ. / С.Г. Чубукова, В.Д. Элькин ; Моск. гос. юрид. акад.; под ред. М.М. Рассолова .— М. : Контракт, 2004 .— 247 с. : ил. — На обл. авт. не указан .— Библиогр. в конце глав .— ISBN 5-900785-84-X.программирование / А.В. Аграновский, Р.А. Хади .— М. : СОЛОН-Пресс, 2002 .— 254, [1] с. : ил.*
3	*Иванов, Михаил Александрович. Криптографические методы защиты информации в компьютерных системах и сетях / Иванов М. А. — М. : Кудиц-Образ, 2001 .— 363 с. : ил.*
4	*Астанин, Иван Константинович. Защита информации : учебное пособие для вузов / И.К.*

	Астанин, Н.И. Астанин ; Воронеж. гос. ун-т, Лискинский филиал .— Воронеж : Воронеж. гос. ун-т, 2006 .— Библиогр. : с.169 .— ISBN 5-9273-1080-х.

* Вначале указываются ЭБС, с которыми имеются договора у ВГУ, затем открытые электронно-образовательные ресурсы

16. Перечень учебно-методического обеспечения для самостоятельной работы

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

№ п/п	Источник
5	*Скоромников, Кир Серафимович. Компьютерное право Российской Федерации : Учебник / К.С.Скоромников;Междунар.независим. эколого-политол.ун-т .— М. : Изд-во МНЭПУ, 2000 .— 220,[1] с. — ISBN 5-7383-0105-6.*
6	*Велпури, Рама. Oracle8i : Резервное копирование и восстановление / Р. Велпури, А. Адколи ; Пер.с англ. И. Афанасьева; Науч. ред. А. Головко; Авт. предислов. Я. Текер .— М. : Лори, 2002 .— 572 с. : ил .— Парал. тит. л. англ. — ISBN 5-85582-166-8.*
7	*Гайдамакин, Н.А. Разграничение доступа к информации в компьютерных системах / Н.А. Гайдамакин .— Екатеринбург : Изд-во Уральского ун-та, 2003 .— 327 с. : ил .— Библиогр.:с.317-322 .— Алф.-предм. указ.: с.306-316 .— ISBN 5-86037-024-5.*
8	*Голуб, Владимир Александрович. Информационная безопасность телекоммуникационных систем : Учебное пособие .— Воронеж : Студия ИАН, 2002 .— 157,[1] с. — ISBN 5-86026-020-2 : 37.00 .— <URL:http://www.lib.vsu.ru/elib/books/b102829.djvu>.*

17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)

Дисциплина может реализовываться с применением электронного обучения и дистанционных образовательных технологий. При проведении занятий в дистанционной форме используются технические и информационные ресурсы Образовательного портала "Электронный университет ВГУ" (https://edu.vsu.ru), базирующегося на системе дистанционного обучения Moodle, развернутой в университете, а также другие доступные ресурсы в сети Интернет.

№ п/п	Источник
1	*www.fstec.ru, www.securitylab.ru , www.cyberpol.ru , www.azi.ru , www.infotecs.ru , www.infosec.ru , www.infoforum.ru , www.cnews.ru , www.brighttalk.com , www.coresecurity.com .*

18. Материально-техническое обеспечение дисциплины:

Компьютеры, с установленным программным обеспечением: Microsoft Visual Studio, LibreOffice.

Для проведения лекционных и лабораторных занятий используются аудитории, соответствующие действующим санитарно-техническим нормам и противопожарным правилам.

Для проведения лабораторных занятий и самостоятельной работы используется класс с компьютерной техникой, оснащенный необходимым программным обеспечением, электронными учебными пособиями и законодательно - правовой и нормативной поисковой системой, имеющий выход в глобальную сеть.

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-1, ОПК-4, ОПК-5	ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-4.2, ОПК-4.3, ОПК-5.1, ОПК-5.2	Домашнее задание, контрольная работа
2	Структура информационных ресурсов. Интеллектуальная собственность и коммерческая тайна.	ОПК-1, ОПК-4, ОПК-5	ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-4.2, ОПК-4.3, ОПК-5.1, ОПК-5.2	Домашнее задание, контрольная работа
3	Угрозы информационной безопасности и их классификация.	ОПК-1, ОПК-4, ОПК-5	ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-4.2, ОПК-4.3, ОПК-5.1, ОПК-5.2	Домашнее задание, контрольная работа
4	Правовые аспекты защиты информации.	ОПК-1, ОПК-4, ОПК-5	ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-4.2, ОПК-4.3, ОПК-5.1, ОПК-5.2	Домашнее задание, контрольная работа
5	Организационные мероприятия, направленные на защиту информации.	ОПК-1, ОПК-4, ОПК-5	ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-4.2, ОПК-4.3, ОПК-5.1, ОПК-5.2	Домашнее задание, контрольная работа
6	Программно-аппаратные средства защиты информации	ОПК-1, ОПК-4, ОПК-5	ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-4.2, ОПК-4.3, ОПК-5.1, ОПК-5.2	Домашнее задание, контрольная работа
7	Математические методы и модели в задачах защиты информации.	ОПК-1, ОПК-4, ОПК-5	ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-4.2, ОПК-4.3, ОПК-5.1, ОПК-5.2	Домашнее задание, контрольная работа
8	Эффективность мероприятий по защите информации	ОПК-1, ОПК-4, ОПК-5	ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-4.2, ОПК-4.3, ОПК-5.1, ОПК-5.2	Домашнее задание, контрольная работа
	Промежуточная аттестация форма контроля – зачёт и экзамен			Перечень вопросов Практическое задание

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Текущая аттестация проводится в форме лабораторных работ и контрольной работы.

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

Собеседование по билетам к зачету

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

Пример КИМ № 1

УТВЕРЖДАЮ
Заведующий кафедрой функционального
анализа и операторных уравнений

_____ Каменский М.И.
подпись, расшифровка подписи

__.__.__

Направление подготовки / специальность ___01.03.04 Прикладная математика_____

Дисциплина_____Б1.В.ДВ.4.1 Защита информации_____

Форма обучения _____очная_____
очное, очно-заочное, заочное

Вид контроля _____зачет_____
экзамен, зачет

Вид аттестации _____промежуточная_____
текущая, промежуточная

Контрольно-измерительный материал № ___

1. Угрозы информационной безопасности.

2. Методы и средства инженерной защиты объектов информатизации

Преподаватель _____ _____.
подпись расшифровка подписи

Пример контрольного задания (вариант задания)

Контрольная работа
по дисциплине «Защита информации»
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.

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 сформированности компетенций	Шкала оценок
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

Задания закрытого типа:

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.

Задания открытого типа:

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.

Задания открытого типа:
1. Вставьте пропущенную часть формулы.
В алгоритме RSA для шифрования сообщения используется следующая формула: $C = M^e[\ldots]n$, где C-полученная криптограмма, M-секретное сообщение, n, e-открытая часть ключа.
Ответ: mod
2. Алгоритм шифрования авторами которого являются Рональд Райвест, Ади Шамир и Леонард Адлеман, стойкость которого основывается на вычислительной сложности задачи факторизации (разложения на множители) больших чисел и задачи дискретного логарифмирования — это алгоритм шифрования ….
Ответ: RSA
Решение: Алгоритм RSA был предложен в 1977 году и стал первым полноценным алгоритмом асимметричного шифрования и электронной

цифровой подписи. Алгоритм назван по первым буквам фамилий авторов – Рональд Райвест (Ronald Rivest), Ади Шамир (Adi Shamir) и Леонард Адлеман (Leonard Adleman).
3. Для криптосистемы RSA модуль *n* является частью открытого ключа и вычисляется следующим образом n=p*q, где p и q - большие […] числа.
Ответ: простые
Решение: Для криптосистемы RSA модуль *n* является частью открытого ключа и вычисляется следующим образом n=p*q, где p и q — большие простые числа.
4. Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления — это …
Ответ: информация
Решение: информация — это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
5. В отличие от симметричных, в асимметричных алгоритмах шифрования используется пара — открытый […] и закрытый […]. Вставьте пропущенное слово.
Ответ: ключ.
Решение: В отличие от симметричных, в асимметричных алгоритмах шифрования используется пара — открытый ключ и закрытый ключ.