МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ
Директор ИЕиС
И.Ю. Мезин

30.01.2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Направление подготовки (специальность)
01.04.02 Прикладная математика и информатика

Направленность (профиль/специализация) программы
Математическое моделирование и цифровые двойники

Уровень высшего образования - магистратура

Форма обучения
очная

Институт/ факультет	Институт естествознания и стандартизации
Кафедра	Прикладной математики и информатики
Курс	2
Семестр	3

Магнитогорск
2023 год

Рабочая программа составлена на основе ФГОС ВО - магистратура по направлению подготовки 01.04.02 Прикладная математика и информатика (приказ Минобрнауки России от 10.01.2018 г. № 13)

Рабочая программа рассмотрена и одобрена на заседании кафедры Прикладной математики и информатики
17.01.2023, протокол № 5

Зав. кафедрой _____ Ю.А. Извеков

Рабочая программа одобрена методической комиссией ИЕиС
30.01.2023 г. протокол № 5

Председатель _____ И.Ю. Мезин

Рабочая программа составлена:
доцент кафедры ПМиИ, канд. пед. наук _____ Т.П. Злыднева

Рецензент:
доцент кафедры Физики, канд. физ.-мат. наук _____ Д.М. Долгушин

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 учебном году на заседании кафедры Прикладной математики и информатики

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ Ю.А. Извеков

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2025 - 2026 учебном году на заседании кафедры Прикладной математики и информатики

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ Ю.А. Извеков

1 Цели освоения дисциплины (модуля)

Целями освоения дисциплины «Информационная безопасность и защита информации» являются:

знание и решение проблемы информационной безопасности;

формирование умений по применению мер обеспечения защиты информации;

получение навыков решения практических задач – построения модели угроз безопасности информации, разработки политики безопасности организации, оценки безопасности информационных технологий;

подготовка студентов к использованию знаний, умений и навыков в практической деятельности и систематическому повышению своего профессионального уровня.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Информационная безопасность и защита информации входит в часть учебного плана формируемую участниками образовательных отношений образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Разработка интернет приложений

Учебная - технологическая (проектно-технологическая)практика

Современные компьютерные технологии

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Производственная - научно-исследовательская работа

Производственная - преддипломная практика

Выполнение и защита выпускной квалификационной работы

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Информационная безопасность и защита информации» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ПК-1 Способность определять первоначальные требования заказчика к ИС и возможности их реализации в ИС на этапе предконтрактных работ	
ПК-1.1	Планирует работы по определению первоначальных требований заказчика к ИС и возможности их реализации в ИС
ПК-1.2	Знает инструменты и методы управления требованиями
ПК-1.3	Владеет методиками описания и моделирования бизнес-процессов, средствами моделирования бизнес-процессов

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 5 зачетных единиц 180 акад. часов, в том числе:

– контактная работа – 54,2 акад. часов:

– аудиторная – 54 акад. часов;

– внеаудиторная – 0,2 акад. часов

– самостоятельная работа – 125,8 акад. часов;

– в форме практической подготовки – 0 акад. час;

Форма аттестации - зачет с оценкой

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Основы информационной безопасности								
1.1 Основные понятия и определения информационной безопасности	3		2		6	Подготовка к лабораторно-практическому занятию Работа с компьютерными обучающими программами, электронными учебниками	Лабораторные работы Тестирование	ПК-1.1, ПК-1.2
1.2 Политика государства в области информационной безопасности			4		6	Работа с электронными учебниками Подбор и описание сайтов Интернет	Тестирование Проверка индивидуальных заданий	ПК-1.1, ПК-1.2
1.3 Угрозы и нарушители безопасности информации			4		8	Подготовка к лабораторно-практическому занятию Работа с электронными учебниками	Лабораторные работы Тестирование	ПК-1.1, ПК-1.2, ПК-1.3
1.4 Модель угроз безопасности информации			2		8	Подготовка к лабораторно-практическому занятию Работа с компьютерными обучающими программами, электронными учебниками	Лабораторные работы Тестирование	ПК-1.1, ПК-1.2, ПК-1.3

1.5 Политика безопасности организации			2		6	Подготовка к лабораторно-практическому занятию Работа с компьютерными обучающими программами, электронными учебниками	Лабораторные работы Тестирование	ПК-1.1, ПК-1.2, ПК-1.3
1.6 Основные стандарты в области информационной безопасности			4		8,8	Работа с электронными учебниками Подбор и описание сайтов Интернет Составление таблиц	Тестирование Проверка индивидуальных заданий	ПК-1.1, ПК-1.2
Итого по разделу			18		42,8			
2. Защита информации								
2.1 Меры обеспечения защиты информации	3		4		10	Подготовка к лабораторно-практическому занятию Работа с компьютерными обучающими программами, электронными учебниками	Лабораторные работы Тестирование	ПК-1.1, ПК-1.2, ПК-1.3
2.2 Организационные меры защиты информации			4		10	Подготовка к лабораторно-практическому занятию Работа с электронными учебниками	Лабораторные работы Тестирование	ПК-1.1, ПК-1.2, ПК-1.3
2.3 Методы контроля и разграничения доступа			6		12	Подготовка к лабораторно-практическому занятию Работа с компьютерными обучающими программами, электронными учебниками	Лабораторные работы Тестирование	ПК-1.1, ПК-1.2, ПК-1.3
2.4 Криптографические методы защиты информации			6		12	Подготовка к лабораторно-практическому занятию Работа с компьютерными обучающими программами, электронными учебниками	Лабораторные работы Тестирование	ПК-1.1, ПК-1.2, ПК-1.3

2.5 Стеганографическая защита информации			4		14	Подготовка к лабораторно-практическому занятию Работа с компьютерными обучающими программами, электронными учебниками	Лабораторные работы Тестирование	ПК-1.1, ПК-1.2, ПК-1.3
2.6 Техническая защита информации. Программно-технические меры защиты информации			6		12	Подготовка к лабораторно-практическому занятию Работа с компьютерными обучающими программами, электронными учебниками	Лабораторные работы Тестирование	ПК-1.1, ПК-1.2, ПК-1.3
2.7 Системы обнаружения и предотвращения компьютерных атак			6		13	Подготовка к лабораторно-практическому занятию Работа с электронными учебниками Составление таблиц	Лабораторные работы Проверка индивидуальных заданий Тестирование	ПК-1.1, ПК-1.2, ПК-1.3
Итого по разделу			36		83			
Итого за семестр			54		125,8		зао	
Итого по дисциплине			54		125,8		зачет с оценкой	

5 Образовательные технологии

В ходе изучения дисциплины «Информационная безопасность и защита информации» рекомендуется использовать образовательные и информационные технологии:

1.Традиционные технологии обучения, предполагающие передачу информации в готовом виде, формирование учебных умений по образцу: лабораторные работы и др.

Использование традиционных технологий обеспечивает ориентирование студента в потоке информации, связанной с различными подходами к определению сущности, содержания, методов, форм развития и саморазвития личности; самоопределение в выборе оптимального пути и способов личностно-профессионального развития; систематизацию знаний, полученных студентами в процессе аудиторной и самостоятельной работы. Лекционные занятия проводятся с использованием мультимедийных средств. Лабораторные занятия обеспечивают развитие и закрепление умений и навыков определения целей и задач саморазвития, а также принятия наиболее эффективных решений по их реализации. Лабораторные занятия проводятся в компьютерных классах вычислительного центра ФГБОУ ВО «МГТУ им. Г.И. Носова».

В ходе проведения лабораторные работ предусматривается использование средств вычислительной техники при выполнении индивидуальных заданий и тестирования.

Текущий и промежуточный контроль осуществляется с использованием средств вычислительной техники.

2. Интерактивные технологии, предполагающие организацию обучения как продуктивной творческой деятельности в режиме взаимодействия студентов друг с другом и с преподавателем. Использование интерактивных образовательных технологий способствует повышению интереса и мотивации учащихся, активизации мыслительной деятельности и творческого потенциала студентов, делает более эффективным усвоение материала, позволяет индивидуализировать обучение и ввести экстренную коррекцию знаний.

3. Информационно-коммуникационные образовательные технологии, предполагающие организацию образовательного процесса, основанную на применении специализированных программных сред и технических средств работы с информацией. Мы используем такие формы учебных занятий с использованием информационно-коммуникационных технологий как практические занятия в форме презентации.

При проведении практических занятий используются групповая работа, технология коллективной творческой деятельности, технология сотрудничества, обсуждение проблемы в форме дискуссии, дебаты. Данные технологии обеспечивают высокий уровень усвоения студентами знаний, эффективное и успешное овладение умениями и навыками в предметной области, формируют познавательную потребность и необходимость дальнейшего самообразования, позволяют активизировать исследовательскую деятельность, обеспечивают эффективный контроль усвоения знаний.

4.Возможности образовательного портала ФГБОУ ВО «МГТУ им. Г.И. Носова» для предоставления студентам графика самостоятельной работы, расписания консультаций, заданий для самостоятельного выполнения и рекомендуемых тем для самостоятельного изучения.

Используемые образовательные технологии позволяют активно применять в учебном процессе интерактивные формы проведения занятий (компьютерная симуляция, разбор конкретных ситуаций), что способствует формированию и развитию

профессиональных навыков обучающихся. Применяемые в процессе изучения дисциплины поисковый и исследовательский методы в полной мере соответствуют требованиям ФГОС по реализации компетентностного подхода.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е. К. Баранова, А. В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2020. — 336 с. — (Высшее образование). - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1114032 (дата обращения: 24.06.2022). – Режим доступа: по подписке

2. Ищейнов, В. Я. Основные положения информационной безопасности : учеб.пособие / В.Я. Ищейнов, М.В. Мецатунян. — Москва : ФОРУМ : ИНФРА-М, 2018. — 208 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-489-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/927190 (дата обращения: 24.06.2022). – Режим доступа: по подписке.

б) Дополнительная литература:

1. Аппаратно-программные средства защиты информации: Практикум / Душкин А.В., Дубровин А.С., Здольник В.В. - Воронеж:Научная книга, 2017. - 198 с.: ISBN 978-5-4446-1043-5. - Текст : электронный. - URL: https://znanium.com/catalog/product/977192 (дата обращения: 24.06.2022). – Режим доступа: по подписке.

2. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е. К. Баранова, А. В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2020. — 320 с. — (Высшее образование). - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/1052206 (дата обращения: 24.06.2022). – Режим доступа: по подписке.

3. Баранова, Е. К. Актуальные вопросы защиты информации : монография / А.В. Бабаш, Е.К. Баранова. — Москва : РИОР : ИНФРА-М, 2020. — 111 с. — (Научная мысль). — https://doi.org/10.12737/monography_58dbc380aa3a4. - ISBN 978-5-369-01680-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1052207 (дата обращения: 24.06.2022). – Режим доступа: по подписке.

4. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/405000 (дата обращения: 24.06.2022). – Режим доступа: по подписке.

5. Введение в информационную безопасность: Учебное пособие для вузов / А.А. Малюк, В.И. Королев, В.М. Фомичев; Под ред. В.С. Горбатов. - Москва : Гор. линия-Телеком, 2011. - 288 с.: ил.; . - (Специальность). ISBN 978-5-9912-0160-5, 1000 экз. - Текст : электронный. - URL: https://znanium.com/catalog/product/265558 (дата обращения: 24.06.2022). – Режим доступа: по подписке.

6. Емельянова, Н. З. Защита информации в персональном компьютере : учебное пособие / Н.З. Емельянова, Т.Л. Партыка, И.И. Попов. — 2-е изд. — Москва : ФОРУМ

: ИНФРА-М, 2020. — 368 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-466-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1058219 (дата обращения: 24.06.2022). – Режим доступа: по подписке.

7. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. - 2-е изд., перераб. и доп. - Москва : ИНФРА-М, 2021. - 256 с. - (Высшее образование:Специалитет). - ISBN 978-5-16-016535-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1178151 (дата обращения: 24.06.2022). – Режим доступа: по подписке.

8. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2021. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1137902 (дата обращения: 24.06.2022). – Режим доступа: по подписке.

9. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П. Б. Хорев. — 3-е изд., испр. и доп. — Москва : ИНФРА-М, 2020. — 327 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-015471-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1035570 (дата обращения: 24.06.2022). – Режим доступа: по подписке.

10. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В. Ф. Шаньгин. — Москва : ФОРУМ :ИНФРА-М, 2020. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1093695 (дата обращения: 24.06.2022). – Режим доступа: по подписке.

в) Методические указания:

Чернова, Е. В. Информационная безопасность : учебное пособие / Е. В. Чернова ; МГТУ. - [2-е изд., подгот. по печ. изд. 2011 г.]. - Магнитогорск : МГТУ, 2015. - 1 электрон.опт. диск (CD-ROM). - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=1453.pdf&show=dcatalogues/1/1123976/1453.pdf&view=true (дата обращения: 24.06.2022). - Макрообъект. - Текст :

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
7Zip	свободно распространяемое ПО	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
Kaspersky Endpoint Security для бизнеса-Стандартный	Д-162-21 от 26.03.2021	26.03.2023

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Электронная база периодических изданий East View Information Services, ООО «ИВИС»	https://dlib.eastview.com/
Национальная информационно-аналитическая система – Российский индекс научного цитирования	URL: https://elibrary.ru/project_risc.asp
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Информационная система - Единое окно доступа к информационным ресурсам	URL: http://window.edu.ru/
Российская Государственная библиотека. Каталоги	https://www.rsl.ru/ru/4readers/catalogues/
Электронные ресурсы библиотеки МГТУ им. Г.И. Носова	http://magtu.ru:8085/marcweb2/Default.asp

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Учебная аудитория для проведения лабораторных работ: компьютерные классы. Оснащение: Персональные компьютеры с пакетом MS Office, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

Помещения для самостоятельной работы обучающихся. Оснащение: Персональные компьютеры с пакетом MS Office, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

Учебные аудитории для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Оснащение: Доска, мультимедийный проектор, экран. Комплекс тестовых заданий для проверки промежуточных и рубежных контролей.

Помещение для хранения и профилактического обслуживания учебного оборудования. Оснащение: Стеллажи для хранения учебно-наглядных пособий и учебно-методической документации.

Приложение1

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Информационная безопасность и защита информации» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.
Аудиторная самостоятельная работа студентов предполагает работу с компьютерными обучающими программами на лабораторно-практических занятиях.
Ко всем изучаемым темам предлагаются тестовые задания, по которым проводится контроль.

Тестовые задания по темам курса:
1.1 Основные понятия и определения информационной безопасности

1) Данными, согласно ГОСТ «Системы обработки информации. Термины и определения», называется информация, представленная в виде, пригодном для обработки:

- Информационными системами под управлением человека
- Автоматизированными системами
- Автоматическими средствами при возможном участии человека
- Средствами вычислительной техники

2) Под электронным сообщением, согласно федеральному закону «Об информации, информационных технологиях и о защите информации», понимается информация:

- Оформленная в виде электронного документа, передаваемого или полученного по сетям связи
- Переданная или полученная пользователем информационно-телекоммуникационной сети
- Представленная в электронном виде, пригодном для передачи при помощи средств вычислительной техники
- Передаваемая по информационно-телекоммуникационной сети с использованием средств вычислительной техники

3) Укажите все действия с информацией, возможность которых, согласно федеральному закону «Об информации, информационных технологиях и о защите информации», получает лицо, которому предоставлен доступ к информации:

- Получение
- Ознакомление
- Распространение
- Использование
- Передача
- Предоставление

4) Укажите все компоненты, входящие, согласно ГОСТ «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения», в понятие «Система обработки информации»:

- Программное обеспечение
- Технические средства
- Действия персонала
- Методы обработки информации

- [ ] Методы хранения информации
- [ ] Методы передачи информации
- [ ] Информационные технологии

5) Укажите все возможные основания для защиты информации, предусмотренные понятием «Защищаемая информация», согласно ГОСТ «Защита информации. Основные термины и определения»:

- [ ] Требования собственника информации
- [ ] Результат экспертной оценки
- [ ] Требования правовых документов
- [ ] Решение суда
- [ ] Соглашение между собственником и пользователем информации

1.2 Политика государства в области информационной безопасности

1) Информационная безопасность, согласно Стратегии национальной безопасности Российской Федерации,

- ○ Является самостоятельным видом безопасности наряду с национальной безопасностью
- ○ Входит в понятие национальной безопасности вместе с другими видами безопасности
- ○ Входит в понятие национальной безопасности вместе с обороной страны и другими видами безопасности
- ○ Входит в понятие национальной безопасности вместе с внешней политикой и другими видами безопасности

2) Система обеспечения информационной безопасности, согласно Доктрине информационной безопасности Российской Федерации, представляет собой совокупность

- ○ Сил обеспечения ИБ, а также средств обеспечения ИБ, управляемых операторами
- ○ Средств обеспечения ИБ и поддерживающих их сил обеспечения ИБ
- ○ Сил обеспечения ИБ и используемых ими средств обеспечения ИБ
- ○ Средств обеспечения ИБ и координирующих их использование сил обеспечения ИБ

3) Укажите все действия, которые, согласно ФЗ «Об информации, информационных технологиях и о защите информации», вправе совершать обладатель информации, если иное не предусмотрено федеральными законами:

- [ ] Определять порядок и условия доступа к информации
- [ ] Передавать информацию другим лицам согласно договору
- [ ] Защищать свои права установленным законом способом в случае использования или получения информации иными лицами
- [ ] Разрешать или ограничивать доступ к информации

4) Необходимым условием для отнесения информации к коммерческой тайне является то обстоятельство, что

- ○ информация носит производственный, технический, экономический или организационный характер
- ○ обладатель информации установил запрет на доступ к ней любых иных лиц
- ○ информация не известна третьим лицам

информация позволяет обладателю увеличить доходы, избежать неоправданных расходов или сохранить положение на рынке товаров, работ, услуг

5) Укажите все принципы обработки персональных данных, предусмотренные ФЗ «О персональных данных»:

- [ ] Обработка максимального набора персональных данных для наиболее точного определения субъекта персональных данных;Определение принципов обработки персональных данных
- [ ] Хранение персональных данных, собранных для достижения каждой цели обработки, строго в отдельных базах данных
- [ ] Обеспечение точности персональных данных
- [ ] Принятие мер по удалению или уточнению неполных или неточных данных
- [ ] Соответствие содержания персональных данных заявленным целям обработки

1.3 Угрозы и нарушители безопасности информации

1) Согласно руководящему документу ФСТЭК России «Защита от несанкционированного доступа к информации. Термины и определения», доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами, называется _____.
2) Укажите порядок следования следующих понятий в логической модели реализации угрозы безопасности информации, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК в 2015 г. В ответе запишите последовательность цифр без запятых и пробелов (например: 1234): 1. Уязвимость; 2. НСД к информации; 3. Угроза; 4. Источник угрозы. _____
3) Выберите все действия, относящееся к основным видам угроз безопасности информации:

- [ ] Распространение информации
- [ ] Разглашение информации
- [ ] Хищение информации
- [ ] Доступ к информации
- [ ] Отрицание подлинности информации
- [ ] Искажение информации

4) Укажите все угрозы, застрагивающие доступность информации:

- [ ] Внесение в исполняемый файл текста вируса
- [ ] Вывод из строя USB носителя
- [ ] Изменение оценки в электронном дневнике
- [ ] Искажение системного файла операционной системы, приводящее к невозможности ее запуска
- [ ] Блокирование учетной записи пользователя в результате компьютерной атаки
- [ ] Отправка сетевых пакетов с поддельным адресом отправителя

5) Выберите все виды нарушителей, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК в 2015 г., относящихся к внутреннему типу:

- [ ] Лица, привлекаемые для установки оборудования

- [ ] Бывший сотрудник организации
- [ ] Сотрудники службы охраны
- [ ] Поставщики оборудования

1.4 Модель угроз безопасности информации

1) Укажите все разделы, входящие в структуру модели угроз безопасности информации, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК в 2015 г.:

- [ ] перечень идентифицированных угроз безопасности информации
- [ ] описание информационной системы
- [ ] оценка ценности информации, содержащейся в информационной системе как актива
- [ ] модель нарушителя
- [ ] перечень актуальных угроз безопасности информации
- [ ] оценка рисков, связанных с идентифицированными угрозами безопасности информации
- [ ] методы защиты от актуальных угроз безопасности информации
- [ ] принятые решения в отношении рисков, связанных с угрозами безопасности информации

2) Укажите порядок следования элементов описания идентифицированных угроз безопасности информации в описации УБИj, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК в 2015 г. В ответе запишите последовательность цифр без запятых и пробелов (например: 12345): 1. Уязвимости информационной системы 2. Объекты воздействия нарушителя 3. Нарушитель (источник угрозы) 4. Последствия от реализации угрозы безопасности информации 5. Способ реализации угрозы. _____

3) Актуальность угрозы, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК в 2015 г., означает, что:

- ○ В информационной системе существует возможность реализации угрозы
- ○ Существует атуальный для данной информационной системы нарушитель с достаточным потенциалом для реализации угрозы
- ○ В информационной системе существует возможность реализации угрозы нарушителем с соответствующим потенциалом и ее реализация приведет к нанесению ущерба
- ○ Реализация угрозы нанесет ущерб владельцу или оператору информации либо субъекту персональных данных
- ○ В информационной системе существует достаточная (средняя или высокая) вероятность реализации угрозы, а ее последствия имеют средний или высокий уровень наносимого ущерба

4) Для оценки возможности реализации угрозы безопасности информации, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК в 2015 г., необходимо учитывать следующие параметры угрозы и информационной системы:

- ○ Уровень защищенности информационной системы, потенциал нарушителя
- ○ Уровень защищенности или проектной защищенности информационной системы, потенциал нарушителя
- ○ Уровень проектной защищенности информационной системы, потенциал нарушителя

- Уровень проектной защищанности информационной системы, потенциал нарушителя или уровень ущерба

5) Реализация угрозы безопасности информации считается, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК в 2015 г., оказывающей воздействие на конкретное свойство безопасности информации, если в результате реализации угрозы безопасности информации:

- Возможны нежелательные действия с информацией, относящиеся к данному свойству безопасности информации
- Нежелательные действия с информацией, относящиеся к данному свойству безопасности информации, имеют достаточную вероятность осущетвления нарушителем
- Нежелательные действия с информацией, относящиеся к данному свойству безопасности информации, имеют высокую вероятность реализации нарушителем
- Неизбежно будут осуществлены нежелательные действия с информацией, относящиеся к данному свойству безопасности информации

1.5 Политика безопасности организации.

1) Укажите все источники законодательных мер защиты информации, распространяющихся на всех участников информационных отношений, в Российской Федерации:

- [ ] указы федеральных органов исполнительной власти
- [ ] приказы уполномоченных федеральных служб
- [ ] распоряжения и приказы министерств РФ
- [ ] международные договоры РФ

2) Разработка политики безопасности предусматривается в рамках

- организационно-технических мер ЗИ
- программно-технических мер ЗИ
- административных мер ЗИ
- морально-этических мер ЗИ

3) Укажите все подсистемы входящие в состав системы обеспечения безопасности информации:

- [ ] Подсистема контроля целостности
- [ ] Подсистема протоколирования и аудита
- [ ] Подсистема антивирусной защиты
- [ ] Подсистема защиты потоков
- [ ] Подсистема контроля доступа

4) Укажите все действия, для совершения которых, согласно определению вредоносной программы из Уголовного кодекса РФ, должна быть заведомо предназначена программа, чтобы считаться вредоносной

- [ ] Несанкционированное распространение информации
- [ ] Несанкционированное уничтожение информации
- [ ] Поиск уязвимостей в ИС
- [ ] Вывод из строя компонентов ИС

- [ ] Нейтрализация средств защиты компьютерной информации

5) Метод обнаружения вредоносных программ, суть которого заключается в поиске участков кода исполняемого объекта, отвечающих за конкретные вредоносные действия, называется

- ○ Комплексным анализом
- ○ Сигнатурным анализом
- ○ Эвристическим анализом
- ○ Методом точного поиска
- ○ Методом эмуляции кода

1.6 Основные стандарты в области информационной безопасности

1) Документ, устанавливающий характеристики продукции, правила осуществления и характеристики процессов, например, производства и эксплуатации, выполнения работ или оказания услуг, называется:

- ○ Государственным стандартом
- ○ Спецификацией
- ○ Техническим заданием
- ○ Стандартом

2) По содержанию стандарты в области информационной безопасности можно разделить на:

- ○ Оценочные стандарты и классификации
- ○ Руководства и методики
- ○ Методики и спецификации
- ○ Оценочные стандарты и спецификации

3) Укажите все криптографические алгоритмы, для которых существуют действующие стандарты Российской Федерации категории Криптографическая защита информации:

- [ ] Поточные шифры
- [ ] Блочные шифры
- [ ] Асимметричные системы шифрования
- [ ] Протокол выработки общего ключа
- [ ] Функция хэширования

4) Государственный стандарт на процессы формирования и проверки электронной цифровой подписи:

- ○ Не предусматривает использования функции хэширования
- ○ Содержит описание функции хэширования, которая должна использоваться при формировании электронной цифровой подписи
- ○ Предусматривает ипользование произвольной функции хэширования по выбору пользователя
- ○ Предусматривает использование функции хэширования, описанной в соответствующем государственном стандарте Российской Федерации

5) ФСТЭК России является уполномоченным органом по вопросам защиты информации:

- Программно-техническими методами
- Организационно-техническими методами
- Организационными методами
- Некриптографическими методами

2.1 Меры обеспечения защиты информации

1) По способам осуществления меры обеспечения защиты информации подразделяются на:

- Законодательные, морально-этические, административные, организационно-технические, программно-технические
- Законодательные, морально-этические, административные, организационные, программно-технические
- Организационные, криптографические, меры технической ЗИ, стеганографические
- Законодательные, морально-этические, административные, организационно-технические

2) Укажите все криптографические методы защиты информации, используемые для обеспечения целостности информации:

- [ ] Системы шифрования
- [ ] Схемы электронной цифровой подписи
- [ ] Контрольные суммы
- [ ] Функции хэширования
- [ ] Взаимная аутентификация абонентов

3) Укажите все угрозы, для защиты от которых меры технической защиты информации рассматриваются как эффективные:

- [ ] Угроза нарушения доступности информации в информационной системе
- [ ] Угроза утечки речевой и видовой информации по техническим каналам
- [ ] Угроза несанкционированного съема информации, обрабатываемой техническими средствами
- [ ] Угроза несанкционированного доступа посторонних лиц в помещения объекта информатизации
- [ ] Угрозы, реализуемые владельцами арендуемых хранилищ данных

4) Любые действующие на территории объекта информатизации правила, регламентирующие доступ к информации и порядок работы с ней, вместе с мерами обеспечения и контроля исполенния таких правил, составляют:

- административные меры ЗИ
- координирующие меры ЗИ
- организационные меры ЗИ
- организационно-технические меры ЗИ

5) Укажите всех нарушителей, для защиты от которых криптографические методы защиты информации рассматриваются как эффективные:

- [ ] Внутренний нарушитель, ответственный за выработку и распространение криптографических ключей

- [ ] Нарушителей, использующих средства несанкционированного получения информации, передаваемой по каналам связи
- [ ] Нарушитель, использующий средства несанкционированного получения информации, обрабатываемой техническими средствами в открытом виде
- [ ] Нарушитель, обладающий значительными вычислительными ресурсами

2.2 Организационные меры защиты информации

1) В задачи организационных мер защиты информации входит

- ○ регламентирование действий посетителей на территории объекта информатизации
- ○ защита от компьютерных атак, осуществляемых по информационно-телекоммуникационным сетям
- ○ создание условий обеспечения и контроля соблюдения регламентов и правил
- ○ противодействие несанкционированному съему информации, обрабатываемой техническими средствами

2) Укажите все мероприятия, которые включают организационно-технические меры ЗИ:

- [ ] Экранирование помещений обработки конфиденциальных сведений
- [ ] Введение пропускного режима на территории предприятия
- [ ] Разработка регламентов действий персонала в чрезвычайных ситуациях
- [ ] Защита объекта информатизации от стихийных угроз

3) По способам осуществления меры обеспечения защиты информации подразделяются на:

- ○ Законодательные, морально-этические, административные, организационно-технические, программно-технические
- ○ Законодательные, морально-этические, административные, организационные, программно-технические
- ○ Организационные, криптографические, меры технической ЗИ, стеганографические
- ○ Законодательные, морально-этические, административные, организационно-технические

4) Укажите все мероприятия, которые включают административные меры защиты информации:

- [ ] Установление пропускного режима на территории предприятия
- [ ] Оценка угроз безопасности информации
- [ ] Обучение и инструктаж персонала
- [ ] Выбор методов и средств защиты информации в организации
- [ ] Защита объекта информатизации от техногенных и стихийных угроз

5) Совокупность людей, процедур и оборудования, защищающих объект информатизации от действий, нарушающих его безопасность представляет собой (выберите один вариант из перечисленных)

- ○ Систему комплексной защиты информации
- ○ Организационно-технические меры защиты информации
- ○ Систему физической защиты
- ○ Программно-технический комплекс защиты информации

2.3 Методы контроля и разграничения доступа

1) Процедура определения тождественности субъекта одному из зарегистрированных в ИС идентификаторов называется: (выберите один вариант из перечисленных)

- Авторизацией
- Верификацией
- Аутентификацией
- Идентификацией

2) В процессе идентификации субъект представляет системе (выберите один вариант из перечисленных)

- Индивидуальный ключ пользователя
- Пароль пользователя
- Идентификатор пользователя

3) Аутентификация – процедура: (выберите один вариант из перечисленных)

- Подтверждения личности пользователем
- Установления подлинности предъявляемой субъектом учетной записи пользователя
- Сопоставления субъекта одному из зарегистрированных идентификаторов
- Установления подлинности предъявляемого субъектом идентификатора

4) Укажите все свойства, характерные для многоразовых паролей: (выберите все подходящие варианты)

- Каждый следующий пароль вырабатывается на основе последовательности предыдущих
- Пароли могут создаваться самим пользователем
- Одной из форм передачи пароля пользователю является короткое сообщение на мобильный телефон
- Пароли могут быть запомнены пользователем
- Эталонный образец пароля запрашивается у пользователя

5) Перечислите все действия, относящиеся к основным задачам разграничения доступа: (выберите все подходящие варианты)

- Обеспечение доступности информации в условиях действия внешнего нарушителя
- Контроль действий пользователя
- Выявление источников внутренних и внешних угроз
- Обеспечение целостности информации
- Минимизация полномочий пользователей
- Выявление аномального поведения пользователей
- Контроль подлинности субъектов после прохождения ими процедуры авторизации

2.4 Криптографические методы защиты информации

1) Укажите все требования, предъявляемые к современным криптографическим системам: (выберите все подходящие варианты)

- Удобство использования

- [ ] Устойчивость к дешифрованию при помощи вычислительной техники
- [ ] Отсуттвие необходимости использовать случайный ключ
- [ ] Возможность стандартизации алгоритмов
- [ ] Устойчивость к навязыванию сообщений

2) В современных блочных шифрах к операциям зашифрования и расшифрования добавляется операция: (выберите один вариант из перечисленных)

- ○ Развертки ключа
- ○ Выработки ключа
- ○ Распределения ключей
- ○ Выработки ключевой пары

3) Отличительной чертой сети Фейстеля по сравнению с SP-сетью является: (выберите один вариант из перечисленных)

- ○ Использование операции «сложение по модулю 2»
- ○ Использование раундовых ключей
- ○ Отсутствие использования S-блоков
- ○ Разделение блока открытого текста на подблоки для зашифрования

4) Надежность криптографической системы RSA основывается на сложности задачи: (выберите один вариант из перечисленных)

- ○ Нахождения обратного элемента конечного поля
- ○ Факторизации (разложения натурального числа на простые множители)
- ○ Возведения элемента конечного поля в степень
- ○ Дискретного логарифмирования

5) Ключевые функции хэширования: (выберите один вариант из перечисленных)

- ○ Не защищают от подделки сообщения
- ○ Используют открытый ключ для проверки
- ○ Используются для аутентификации автора сообщения
- ○ Используются для проверки целостности сообщения

6) Наиболее распространенной схемой совместного использования симметричных и асимметричных систем шифрования является использование: (выберите один вариант из перечисленных)

- ○ Симметричной системы для шифрования сообщений, целостность и авторство которых подтверждаются электронной цифровой подписью
- ○ Симметричной системы для шифрования менее важной информации, асимметричной – для шифрования особо важных сообщений
- ○ Симметричных систем шифрования для связи внутри устойчивых групп абонентов, асимметричных систем – для связи с абонентами, не входящими в такие группы
- ○ Симметричной системы для шифрования сообщений, ключ которой передается при помощи асимметричной системы

2.5 Стеганографическая защита информации

1) Укажите все примеры применения стеганографической защиты информации: (выберите все подходящие варианты)

- [ ] Использование шифра «решетка Кардано»
- [ ] Использование шифровального устройства «сцитала»
- [ ] Написание текста на редком языке
- [ ] Использование приемов каллиграфии

2) Объединение методов и средств, используемых для создания скрытого канала передачи информации называется: (выберите один вариант из перечисленных)

- ○ Стеганографической системой
- ○ Стеганографическим каналом
- ○ Стеганографическим средством
- ○ Стеганографической средой

3) Навязывать те или иные действия абонентам стеганографической системы нарушитель может, реализуя угрозу (выберите один вариант из перечисленных)

- ○ Подмены стеганографического контейнера
- ○ Подмены скрытого сообщения
- ○ Разрушения скрытого сообщения
- ○ Разрушения стеганографического контейнера

4) Активным называется нарушитель безопасности стеганографической системы, который имеет возможность (выберите один вариант из перечисленных)

- ○ Модифицировать, комбинировать, а также подделывать пересылаемые сообщения
- ○ Просматривать, активно изучать, копировать и сопоставлять пересылаемые сообщения
- ○ Активно влиять на работу стеганографической системы, на возможность абонентов создавать, отправлять и получать сообщения
- ○ Просматривать сообщения, модифицировать их без изменения видимой семантической части

5) Высокой эффективностью по критерию отношения сигнал-шум обладает (выберите один вариант из перечисленных)

- ○ Четное кодирование
- ○ Фазовое кодирование
- ○ Метод расширенного спектра
- ○ Эхо-метод встраивания сообщений

2.6 Техническая защита информации. Программно-технические меры защиты информации

1) Понятия «технические средства обработки информации» и «средства вычислительной техники» связаны следующим образом: (выберите один вариант из перечисленных)

- ○ Означают различные, не имеющие пересечений категории объектов
- ○ Средства вычислительной техники – одна из категорий технических средств обработки информации
- ○ Являются синонимами, означая почти совпадающие категории объектов
- ○ Технические средства обработки информации – одна из категорий средств

2) Технический канал утечки информации характеризуется тем, что: (выберите один вариант из перечисленных)

- Злоумышленник использует техническое средство съема информации
- Распространение информации связано с работой технических средств;
- Передаваемая информация пригодна для восприятия только техническими средствами
- Источником информации является техническое средство обработки информации

3) Паразитные электромагнитные связи и наводки является причиной возникновения: (выберите один вариант из перечисленных)

- Содержащих информацию излучений вокруг звукоусилительной аппаратуры
- Содержащих информацию излучений вокруг вычислительной техники
- Содержащих информацию сигналов в неинформационных линиях и цепях
- Содержащих информацию радиосигналов, распространяющихся в пространстве

4) Метод нейтрализации технических каналов утечки информации, заключающийся в отделении источника информации от среды распространения непреодолимым для носителя информации барьером, называется: (выберите один вариант из перечисленных)

- Экранированием
- Ограничением
- Локализацией
- Изолированием

5) Укажите все действия, включаемые в понятие антивирусной защиты, согласно методическим документам ФСТЭК, содержащих профили защиты САВЗ:

- Препятствование «заражению» объектов в ИС
- Обнаружение вредоносных компьютерных программ
- Изолирование вредоносных компьютерных программ
- Удаление «зараженных» объектов
- Блокирование «зараженных» объектов

2.7 *Системы обнаружения и предотвращения компьютерных атак*

1) Основным назначением систем обнаружения и предотвращения компьютерных атак является:

- Минимизация вероятности успешной реализации атаки нарушителем
- Выявление нарушений политики безопасности организации
- Выявление действий нарушителей безопасности информации, информирование о таких действиях
- Исключение возможности реализации компьютерной атаки нарушителем

2) Укажите все уязвимости, присущие любой системе контроля и разграничения доступа на основе принципов ее работы:

- Предусматривают предоставление прав доступа субъектам одновременно к группам сходных объектов
- Не контролируют действия пользователя в рамках его полномочий в системе после успешного прохождения авторизации

- [ ] Не имеют механизмов ограничения прав привилегированного пользователя системы
- [ ] Допускают ошибочное успешное прохождение процедуры аутентификации
- [ ] Не позволяют индивидуально настроить права доступа к объектам для каждого пользователя

3) Укажите все результаты, достижение которых может обеспечить использование систем обнаружения и предотвращения компьютерных атак:

- [ ] Полное исключение возможности успешной реализации компьютерной атаки
- [ ] Полная автоматизация обнаружения попыток реализации компьютерных атак
- [ ] Обнаружение уязвимых настроек, ошибок конфигурации узлов АС
- [ ] Автоматизация обнаружения известных атак на основе сигнатур
- [ ] Компенсация уязвимостей, систем аутентификации пользователей

4) Согласно классификации систем обнаружения и предотвращения компьютерных атак, после завершения атаки действуют:

- ○ Системы анализа журналов регистрации
- ○ Системы обнаружения вторжений
- ○ «Классические» системы обнаружения атак
- ○ Системы анализа защищенности

5) Укажите все варианты размещения сенсоров сетевой системы обнаружения атак, при которых трафик между локальной сетью и сетью Интернет не контролируется:

- [ ] Перед маршрутизатором
- [ ] В демилитаризованной зоне
- [ ] Между маршрутизатором и межсетевым экраном
- [ ] У сервера удаленного доступа
- [ ] За межсетевым экраном

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде изучения литературы по соответствующему разделу с проработкой материала, подготовки к лабораторно-практическим занятиям, выполнения индивидуальных заданий (составление таблиц, подбор и описание сайтов Интернет)

Подготовка к лабораторно-практическим занятиям проводится в соответствии с заданиями, представленными на образовательном портале ФГБОУ ВО «МГТУ им. Г.И. Носова».

Индивидуальные задания:

составление таблиц – по темам «Основные стандарты в области информационной безопасности», «Системы обнаружения и предотвращения компьютерных атак»;

подбор и описание сайтов Интернет – по теме «Основные стандарты в области информационной безопасности», «Политика государства в области информационной безопасности».

Приложение 2

7 Оценочные средства для проведения промежуточной аттестации

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Код индикатора	Индикатор достижения компетенции	Оценочные средства
ПК-1 Способность определять первоначальные требования заказчика к ИС и возможности их реализации в ИС на этапе предконтрактных работ		
ПК-1.1	Планирует работы по определению первоначальных требований заказчика к ИС и возможности их реализации в ИС	***Практические задания*** 1. Подготовить таблицу " Пакеты антивирусных программ ", используя любые доступные источники информации. 2. Используя один из алгоритмов симметричного шифрования, зашифровать свои данные: фамилию, имя, отчество. Выполнить проверку, расшифровав полученное сообщение. 3. Разработать программу, представляющую собой форму доступа к определённым информационным ресурсам на основе пароля: в качестве информационного ресурса использовать любой файл или приложение. 4. Сформировать электронно-цифровую подпись к сообщению (согласно варианту) и произвести проверку целостности принятого сообщения. 5. Разработать программу имитирующую некоторые (согласно варианту) действия по предупреждению вирусных угроз, обнаружению и удалению вирусных и других вредоносных программ и подготовить отчет о проделанной работе.
ПК-1.2	Знает инструменты и методы управления требованиями	***Контрольный тест*** 1) Укажите все варианты того, что может являться объектом защиты информации, предусмотренные ГОСТ «Защита информации. Основные термины и определения»: ☐ Информация ☐ Носитель информации ☐ Система обработки информации ☐ Информационная технология ☐ Информационный процесс

		2) Укажите все принципы, в соответствии с которыми, согласно закону «О государственной тайне», осуществляется отнесение сведений к государственной тайне и их засекречивание: ☐ Своевременности ☐ Законности ☐ Обоснованности ☐ Целесообразности ☐ Необходимости ☐ Допустимости ☐ Справедливости 3) Укажите порядок следования следующих понятий в логической модели реализации угрозы безопасности информации, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК в 2015 г. В ответе запишите последовательность цифр без запятых и пробелов (например: 1234): 1. Уязвимость; 2. НСД к информации; 3. Угроза; 4. Источник угрозы. _____ 4) Укажите все криптографические алгоритмы, для которых существуют действующие стандарты Российской Федерации категории Криптографическая защита информации: ☐ Поточные шифры ☐ Блочные шифры ☐ Асимметричные системы шифрования ☐ Протокол выработки общего ключа ☐ Функция хэширования 5) Укажите все подсистемы входящие в состав системы обеспечения безопасности информации: ☐ Подсистема контроля целостности ☐ Подсистема протоколирования и аудита ☐ Подсистема антивирусной защиты

		☐ Подсистема защиты потоков ☐ Подсистема контроля доступа 6) Укажите все угрозы, для защиты от которых меры технической защиты информации рассматриваются как эффективные: ☐ Угроза нарушения доступности информации в информационной системе ☐ Угроза утечки речевой и видовой информации по техническим каналам ☐ Угроза несанкционированного съема информации, обрабатываемой техническими средствами ☐ Угроза несанкционированного доступа посторонних лиц в помещения объекта информатизации ☐ Угрозы, реализуемые владельцами арендуемых хранилищ данных 7) Укажите все примеры применения стеганографической защиты информации: (выберите все подходящие варианты) ☐ Использование шифра «решетка Кардано» ☐ Использование шифровального устройства «сцитала» ☐ Написание текста на редком языке ☐ Использование приемов каллиграфии 8) Укажите все действия, включаемые в понятие антивирусной защиты, согласно методическим документам ФСТЭК, содержащих профили защиты САВЗ: ☐ Препятствование «заражению» объектов в ИС ☐ Обнаружение вредоносных компьютерных программ ☐ Изолирование вредоносных компьютерных программ ☐ Удаление «зараженных» объектов ☐ Блокирование «зараженных» объектов
ПК-1.3	Владеет методиками описания и моделирования	***Контрольный тест***

	бизнес-процессов, средствами моделирования бизнес-процессов	1) Угроза безопасности информации, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК в 2015 г., называется целенаправленной, если ○ угроза направлена на конкретную информационную систему ○ источником угрозы является человек, действующий преднамеренно ○ в результате реализации угрозы владельцу информационной системы наносится материальный ущерб ○ в результате реализации угрозы нарушитель получает материальную или иную выгоду 2) Реализация угрозы безопасности информации считается, согласно Методике определения угроз безопасности информации в информационных системах, разработанной ФСТЭК в 2015 г., оказывающей воздействие на конкретное свойство безопасности информации, если в результате реализации угрозы безопасности информации: ○ Возможны нежелательные действия с информацией, относящиеся к данному свойству безопасности информации ○ Нежелательные действия с информацией, относящиеся к данному свойству безопасности информации, имеют достаточную вероятность осуществления нарушителем ○ Нежелательные действия с информацией, относящиеся к данному свойству безопасности информации, имеют высокую вероятность реализации нарушителем ○ Неизбежно будут осуществлены нежелательные действия с информацией, относящиеся к данному свойству безопасности информации 3) По способам осуществления меры обеспечения защиты информации подразделяются на: ○ Законодательные, морально-этические, административные, организационно-технические, программно-технические ○ Законодательные, морально-этические, административные, организационные, программно-технические ○ Организационные, криптографические, меры технической ЗИ, стеганографические ○ Законодательные, морально-этические, административные,

		организационно-технические 4) В процессе идентификации субъект представляет системе (выберите один вариант из перечисленных) ○ Индивидуальный ключ пользователя ○ Пароль пользователя ○ Идентификатор пользователя 5) Надежность криптографической системы RSA основывается на сложности задачи: (выберите один вариант из перечисленных) ○ Нахождения обратного элемента конечного поля ○ Факторизации (разложения натурального числа на простые множители) ○ Возведения элемента конечного поля в степень ○ Дискретного логарифмирования 6) Навязывать те или иные действия абонентам стеганографической системы нарушитель может, реализуя угрозу (выберите один вариант из перечисленных) ○ Подмены стеганографического контейнера ○ Подмены скрытого сообщения ○ Разрушения скрытого сообщения ○ Разрушения стеганографического контейнера 7) Технический канал утечки информации характеризуется тем, что: (выберите один вариант из перечисленных) ○ Злоумышленник использует техническое средство съема информации ○ Распространение информации связано с работой технических средств; ○ Передаваемая информация пригодна для восприятия только техническими средствами ○ Источником информации является техническое средство обработки информации 8) Основным назначением систем обнаружения и предотвращения компьютерных атак является:

		Минимизация вероятности успешной реализации атаки нарушителем Выявление нарушений политики безопасности организации Выявление действий нарушителей безопасности информации, информирование о таких действиях Исключение возможности реализации компьютерной атаки нарушителем

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Промежуточная аттестация по дисциплине «Информационная безопасность и защита информации» включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений.

Промежуточная аттестация по данной дисциплине проводится в форме зачета с оценкой. Зачет проводится в форме итогового тестирования по теоретическому материалу и выполнения итогового практического задания на компьютере. К итоговому тестированию допускаются только те студенты, которые отчитались по всем формам текущего контроля (лабораторные работы, текущее тестирование – каждое тестовое задание должно быть выполнено не менее чем на 50 %). По результату выполнения итогового тестового задания выставляется оценка. Оценка по промежуточной аттестации зависит от результатов текущего контроля, оценки за итоговое тестовое задание и оценки за итоговое практическое задание.

Перечень тем для подготовки к зачету:

1. Основы информационной безопасности. Основные понятия и определения
2. Политика государства в области информационной безопасности
3. Угрозы и нарушители безопасности информации.
4. Модель угроз безопасности информации
5. Меры обеспечения защиты информации
6. Организационные меры защиты информации
7. Методы контроля и разграничения доступа
8. Исторический обзор криптографических методов защиты информации
9. Криптографические методы защиты информации
10. Стеганографическая защита информации
11. Техническая защита информации
12. Программно-технические меры защиты информации
13. Политика безопасности организации
14. Системы обнаружения и предотвращения компьютерных атак
15. Основные стандарты в области информационной безопасности

Итоговое тестовое задание содержит 30 теоретических вопросов, каждый правильный ответ оценивается в 1 балл. Критерий оценивания итогового теста:

- на оценку *«отлично»* – 25-30 баллов;
- на оценку *«хорошо»* – 20-24 баллов;
- на оценку *«удовлетворительно»* – 10-19 баллов;
- на оценку *«неудовлетворительно»* – менее 10 баллов.

Итоговое практическое задание представляет собой комплексное задание, которое необходимо выполнить на компьютере. Оценивание практического задания: *зачтено* или *не зачтено*

Показатели и критерии оценивания зачета:

– на оценку *«отлично»* студент демонстрирует высокий уровень сформированности компетенций, показывает высокий уровень знаний не только на уровне воспроизведения и объяснения теоретической информации, но и интеллектуальные навыки по обеспечению информационной безопасности и защите информации, нахождения уникальных ответов к

проблемам, свободно выполняет практические задания, свободно оперирует знаниями, умениями, применяет их в ситуациях повышенной сложности;

– на оценку *«хорошо»* студент демонстрирует средний уровень сформированности компетенций, показывает знания не только на уровне воспроизведения и объяснения информации, но и хорошие навыки по обеспечению информационной безопасности и защите информации: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации;

– на оценку *«удовлетворительно»* студент демонстрирует пороговый уровень сформированности компетенций, показывает знания на уровне воспроизведения и объяснения информации, навыки выполнения простейших заданий по обеспечению информационной безопасности и защите информации, проявляется отсутствие отдельных знаний, умений, навыков, обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации;

– на оценку *«неудовлетворительно»*студент не может показать знания на уровне воспроизведения и объяснения информации, не может показать навыки обеспечению информационной безопасности и защите информации.