Министерство образования Московской области
Государственное образовательное учреждение
высшего образования Московской области
«Государственный гуманитарно-технологический университет»

УТВЕРЖДАЮ
проректор
_____ /Егорова Г.В.__/
«31» августа 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.02 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки	**44.04.01 Педагогическое образование**
Направленность (профиль) программы	**Использование информационных технологий в общем образовании**
Квалификация выпускника	**Магистр**
Форма обучения	**Очная**

Орехово-Зуево
2023 г.

1. Пояснительная записка

Рабочая программа дисциплины составлена на основе учебного плана 44.04.01 Педагогическое образование по профилю Использование информационных технологий в общем образовании 2023 года начала подготовки.

При реализации образовательной программы университет вправе применять дистанционные образовательные технологии.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Цели дисциплины

Цель изучения дисциплины «Информационная безопасность» - формирование у обучающихся базовых теоретических знаний в области информационной безопасности и развитие необходимых практических умений и навыков их применения в будущей профессиональной деятельности.

Задачи дисциплины

- сформировать общее представление об информационной безопасности, как о состоянии защищенности информационного ресурса сложной системы, понимание необходимости системного подхода к практической реализации такого состояния;
- передать знания о порядке организации и практической реализации типовых мероприятий по обеспечению информационной безопасности и защите информации;
- привить навыки анализа информационных ресурсов по следующим факторам: важность, конфиденциальность, уязвимость.

Знания и умения обучающегося, формируемые в результате освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

В результате изучения дисциплины «Информационная безопасность» студент должен обладать следующими компетенциями:	**Коды формируемых компетенций**
Специальные профессиональные компетенции (СПК):	
- способен реализовывать образовательные программы в соответствии с требованиями федеральных государственных образовательных стандартов.	ПК-1

Индикаторы достижения компетенций

Код и наименование компетенции	Наименование индикатора достижения компетенции
ПК-1 способен реализовывать образовательные программы в соответствии с требованиями федеральных государственных образовательных стандартов	**ПК-1.1.** **Знает:** преподаваемый предмет; психолого-педагогические основы и современные образовательные технологии; особенности организации образовательного процесса в соответствии с требованиями образовательных стандартов; **ПК-1.2.** **Умеет:** использовать педагогически обоснованные формы, методы и приемы организации деятельности обучающихся; применять современные образовательные технологии; создавать образовательную среду, обеспечивающую формирование у обучающихся образовательных результатов, предусмотренных ФГОС и (или) образовательными стан-

	дартами, установленными образовательной организацией, и (или) образовательной программой; **ПК-1.3.** **Владеет**: навыками профессиональной деятельности по реализации программ учебных дисциплин.

3. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Б1.В.02 «Информационная безопасность» относится к части, формируемой участниками образовательных отношений блока 1. Дисциплины (модули).

Программа курса предполагает наличие у студентов знаний по всем разделам Высшей математики и Информатики.

4. Структура и содержание дисциплины

Очная форма обучения

№ п/п	Раздел/тема	Семестр	Всего час.	Виды учебных занятий			Промежуточная аттестация
				Контактная работа		СРС	
				Лекции	ПЗ		
	Модуль 1. Основные положения теории информационной безопасности	1	30	2	8	20	
1.	Тема 1. Общие проблемы безопасности. Основные положения теории информационной безопасности	1	15	1	4	10	
2.	Тема 2. Нормативно-правовые аспекты информационной безопасности и защиты информации	1	15	1	4	10	
	Модуль 2. Защита информации	1	42	2	12	28	
3.	Тема 3. Административно-организационные аспекты информационной безопасности и защиты информации	1	21	1	6	14	
4.	Тема 4. Защита информации в информационных системах	1	21	1	6	14	
	Промежуточная аттестация - зачет	1	0	0	0	0	
Итого в 1 семестре			72	4	20	48	

Содержание дисциплины структурированное по темам (разделам)

1 семестр

Лекции

Модуль 1. Основные положения теории информационной безопасности

Лекция 1. Общие проблемы безопасности. Основные положения теории информационной безопасности

Основные понятия информационной безопасности (ИБ). Понятие тайны как объекта защиты ИБ. Организация защиты информации (ЗИ). Политика ИБ. Субъекты и сред-

ства, представляющие угрозу для ИБ. Субъекты и средства, осуществляющие защиту информации.

Лекция 2. Нормативно-правовые аспекты информационной безопасности и защиты информации

Организационная защита информации. Работа с конфиденциальной информацией. Функции службы безопасности. Классификация способов защиты информации. Основные действия по защите информации. Процессы создания и эксплуатации системы информационной безопасности. Типовая модель многорубежной системы защиты информации.

Модуль 2. Защита информации

Лекция 3. Административно-организационные аспекты информационной безопасности и защиты информации

Организационная защита информации. Работа с конфиденциальной информацией. Функции службы безопасности. Классификация способов защиты информации. Основные действия по защите информации. Процессы создания и эксплуатации системы информационной безопасности. Типовая модель многорубежной системы защиты информации.

Лекция 4. Защита информации в информационных системах

Основные принципы организации процесса защиты информации. Угрозы информационной безопасности. Средства защиты информации. Защита информации от утечки по техническим каналам. Оценка эффективности системы ИБ. Средства несанкционированного доступа и защиты аудио информации. Средства несанкционированного доступа и защиты видео информации.

Практические занятия

Модуль 1. Основные положения теории информационной безопасности

Практические занятия 1-2.
Тема «Общие проблемы безопасности. Основные положения теории информационной безопасности»
Учебные цели: ввести основные понятия информационной безопасности (ИБ). Рассмотреть общие проблемы ИБ и организации защиты информации (ЗИ).
Основные термины и понятия:
- информационная безопасность,
- защита информации.

Практические занятия 3-4.
Тема «Нормативно-правовые аспекты информационной безопасности и защиты информации»
Учебные цели: ознакомить студентов с основными нормативными актами и конституционными нормами в сфере информации в Российской Федерации. Объяснить права и обязанности обладателя информации.
Основные термины и понятия:
- нормативные акты в сфере информации
- права и обязанности обладателя информации
- информационные технологии

Модуль 2. Защита информации

Практические занятия 5-7.
Тема «Административно-организационные аспекты информационной безопасности и защиты информации»

Учебные цели: рассмотреть общие проблемы организации защиты информации, работы с конфиденциальной информацией, процессы создания и эксплуатации системы информационной безопасности

Основные термины и понятия:

- конфиденциальная информация;
- организационная защита;
- инженерно-техническая защита.

Практические занятия 8-10.

Тема «Защита информации в информационных системах»

Учебные цели: объяснить студентам основные принципы организации процесса защиты информации. Рассмотреть основные угрозы информационной безопасности и средства защиты информации.

Основные термины и понятия:

- угроза конфиденциальности информации;
- утечка информации

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Для организации самостоятельной работы обучающихся используется основная и дополнительная литература.

Перечень литературы для организации самостоятельной работы:

1. Ефремов, И.В. Информационные технологии в сфере безопасности: практикум : учебное пособие / И.В. Ефремов, В.А. Солопова ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Оренбургский государственный университет». - Оренбург : ОГУ, 2013. - 116 с. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=259178

2. 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. - Библиогр.: с. 221-226 - ISBN 978-5-4475-9823-5; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=499170

Содержание самостоятельной работы студентов:

При выполнении заданий необходимо использовать: материалы аудиторных занятий; методики полученные на практических занятиях; основную и дополнительную литературу.

Модуль 1. Основные положения теории информационной безопасности

Задание 1:

Подготовить реферат по одной из следующих тем:

1. Три вида возможных нарушений информационной безопасности.
2. 3 составляющих ИБ: целостность, доступность, конфиденциальность.
3. Защита информационной системы от угроз.

Рекомендации: Реферирование – это процесс мысленной переработки письменного или устного изложения читаемого текста, результатом которого является составление вторичного документа – реферата. Цель реферата – в наиболее краткой форме передать содержание подлинника, но выделить особо важное или новое, что содержится в реферируемом материале.

Задание 2:

Подготовить доклад на одну из следующих тем:

1. Понятие нарушителя информационной безопасности.

2. Хакеры. Виды хакеров. Примеры хакерских атак.
3. Вирусы как класс вредоносного программного обеспечения. Виды вирусов и их классификация.

Рекомендации:

Этапы подготовки доклада

1. Подготовка и планирование.
2. Выбор и осознание темы доклада.
3. Подбор источников и литературы.
4. Работа с выбранными источниками и литературой.
5. Систематизация и анализ материала.
6. Составление рабочего плана доклада.
7. Письменное изложение материала по параграфам.
8. Редактирование, переработка текста.
9. Оформление доклада.
10. Выступление с докладом.

Структура и доклада, как правило, индивидуальна и зависит от особенностей научной работы и ее темы, однако традиционно включает в себя следующие части.

1. Титульный лист.

2. План (оглавление, содержание). В нем последовательно излагаются названия пунктов доклад (простой план). Доклад может структурироваться по главам и параграфам (сложный план). Здесь необходимо указать номера страниц, с которых начинается каждый пункт плана. Каждая глава начинается с новой страницы. Заголовки каждой главы, параграфа печатаются в середине строчки, в конце заголовка точка не ставится. Не допускаются кавычки и переносы слов.

3. Вводная часть (введение). Формулируется тема доклада, определяется место рассматриваемой проблематики среди других научных проблем и подходов, т.е. автор объясняет ее актуальность и значимость. Даётся краткий обзор источников, на материале которых раскрывается тема.

Далее раскрывают цель (например, показ разных точек зрения, разных подходов на определенную личность или явление, событие) и задачи (в качестве задач можно давать описание позиций авторов, раскрывать различные стороны деятельности).

4. Основная часть. Структурируется по главам, параграфам, количество и названия которых определяются автором и руководителем. Основной материал излагается в форме связного, последовательного, доказательного повествования, иллюстрация автором основных положений. Подбор материала в основной части доклада должен быть направлен на рассмотрение и раскрытие основных положений выбранной темы; выявление собственного мнения обучающегося, сформированного на основе работы с источниками и литературой.

Обязательными являются ссылки на авторов, чьи позиции, мнения, информация использованы в докладе/реферате. Оформляются ссылки и цитаты в соответствии с правилами. Ссылки могут быть двух видов: внутритекстовые и подстрочные.

Модуль 2. Защита информации

Задание 1:

Выполнить анализ различных способов нарушений информационной безопасности (хакерские атаки, отказы оборудования в обслуживании, внешние факторы, влияющие прямо на информационную безопасность систем). Результат представить в виде доклада с мультимедийной презентацией.

Рекомендации к выполнению:

Дидактические требования к составлению мультимедийных презентаций:

1. Должна быть строго определена тема презентации.
2. Презентация должна включать от 10 до 17 слайдов. При этом следует помнить, что активно воспринимаются не более 5-7 слайдов.

3. Первый слайд должен содержать название презентации.
4. Слайды презентации должны содержать фактическую и иллюстративную информацию.
5. Фактическую информацию желательно подавать в виде схем, таблиц, кратких цитат и изречений.
6. Иллюстративная информация может быть в виде графиков, диаграмм, репродукций.
7. Презентация может содержать видео фрагмент продолжительностью до 3-5 минут, во многом дополняющий или иллюстрирующий ранее предложенную информацию.
8. Презентация должна представлять собой целостную логически связанную последовательность слайдов.
9. Обязательно последние слайды презентации должны подводить итог, делать вывод или наводить на самостоятельное размышление.
10. Использование презентации должно сопровождаться комментариями, которые должны дополняться или конкретизироваться содержанием слайдов. Фактическая информация слайдов не должна дублироваться устным выступлением или подменять его.

Задание 2:

Подготовить сообщение по одной из следующих тем:

1. Криптография, криптоанализ.
2. Основные понятия криптологии.
3. История шифрования.
4. Методы шифрования.
5. Метод Винжера.
6. Программная реализация криптографии.
7. Электронная цифровая подпись.

6. Фонд оценочных средств для проведения текущего контроля знаний, промежуточной аттестации обучающихся по дисциплине

Фонд оценочных средств для проведения текущего контроля знаний, промежуточной аттестации приведен в приложении.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

7.1. Перечень основной литературы:

1. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-9585-0603-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=438331

7.2. Перечень дополнительной литературы:

1. Ефремов, И.В. Информационные технологии в сфере безопасности: практикум : учебное пособие / И.В. Ефремов, В.А. Солопова ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Оренбургский государственный университет». - Оренбург : ОГУ, 2013. - 116 с. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=259178

2. 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. - Библиогр.: с. 221-226 - ISBN 978-5-4475-9823-5; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=499170

8. Перечень современных профессиональных баз данных, информационных справочных систем

Все обучающиеся обеспечены доступом к современным профессиональным базам данных и информационным справочным системам, которые подлежат обновлению при необходимости, что отражается в листах актуализации рабочих программ.

Современные профессиональные базы данных:

1. http://информатика.1сентября.рф/2007/12/00.htm Энциклопедия учителя информатики
2. www.edu.ru Федеральный портал "Российское образование"
3. fcior.edu.ru Федеральный центр информационно-образовательных ресурсов
4. https://www.intuit.ru/studies/courses/1031/242/info НОУ ИНТУИТ, курс «Введение в теорию автоматов»
5. https://vk.com/videos-30558759?section=album_3 Лекторий Минобрнауки / Минпросвещения России
6. https://www.intuit.ru/studies/courses/2256/140/info НОУ ИНТУИТ, курс «Основы теории информации и криптографии»
7. http://kvant.mccme.ru/ - Полный электронный архив научно-популярного физико-математического журнала «Квант» (1970–2008 гг.)

Электронные библиотеки:

ЭБС «Университетская библиотека ONLINE»: http://biblioclub.ru.
ЭБС «IPRbooks»: http://www.iprbookshop.ru/
ЭБС «BOOK.ru»: https://www.book.ru/
ЭБС «Консультант студента»: http://www.studmedlib.ru/
База научных статей издательства «Грамота»: http://www.gramota.net/
http://www.google.ru/
http://www.yandex.ru/

9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для осуществления образовательного процесса по дисциплине имеется в наличии следующая материально-техническая база:

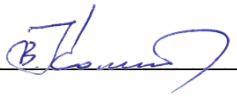
Аудитории	Программное обеспечение
- учебная аудитория для проведения учебных занятий по дисциплине, оснащенная компьютером с выходом в интернет, мультимедиа проектором; - помещение для самостоятельной работы обучающихся, оснащенное компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду ГГТУ; - специализированная аудитория для проведения лабораторных работ по дисциплине, оснащенная набором реактивов и лабораторного оборудования.	Операционная система Пакет офисных приложений Браузер Firefox, Яндекс

10. Обучение инвалидов и лиц с ограниченными возможностями здоровья

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья. Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).

Авторы (составители):  к.ф.-м.н., доц. Русаков О.В.

Программа одобрена на заседании кафедры информатики и физики
от 29 августа 2023 г. Протокол № 1.

И. о. зав. кафедрой информатики и физики  Компанеец В.Н.

Приложение 1.

Министерство образования Московской области
Государственное образовательное учреждение высшего образования
Московской области
«Государственный гуманитарно-технологический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Б1.В.02 Информационная безопасность

Направление подготовки	**44.04.01 Педагогическое образование**
Направленность (профиль) программы	**Использование информационных технологий в общем образовании**
Квалификация выпускника	**Магистр**
Форма обучения	**Очная**

Орехово-Зуево
2023 г.

1. Индикаторы достижения компетенций

Код и наименование компетенции	Наименование индикатора достижения компетенции
ПК-1 способен реализовывать образовательные программы в соответствии с требованиями федеральных государственных образовательных стандартов	**ПК-1.1.** **Знает:** преподаваемый предмет; психолого-педагогические основы и современные образовательные технологии; особенности организации образовательного процесса в соответствии с требованиями образовательных стандартов; **ПК-1.2.** **Умеет:** использовать педагогически обоснованные формы, методы и приемы организации деятельности обучающихся; применять современные образовательные технологии; создавать образовательную среду, обеспечивающую формирование у обучающихся образовательных результатов, предусмотренных ФГОС и (или) образовательными стандартами, установленными образовательной организацией, и (или) образовательной программой; **ПК-1.3.** **Владеет**: навыками профессиональной деятельности по реализации программ учебных дисциплин.

2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Оценка уровня освоения компетенций на разных этапах их формирования проводится на основе дифференцированного контроля каждого показателя компетенции в рамках оценочных средств, приведенных в ФОС.

Оценка «Отлично», «Хорошо», «Зачтено» соответствует повышенному уровню освоения компетенции согласно критериям оценивания, приведенных в таблице к соответствующему оценочному средству.

Оценка «Удовлетворительно», «Зачтено» соответствует базовому уровню освоения компетенции согласно критериям оценивания, приведенных в таблице к соответствующему оценочному средству.

Оценка «Неудовлетворительно», «Не зачтено» соответствует показателю «компетенция не освоена».

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде	Критерии оценивания
Оценочные средства для проведения текущего контроля				
1.	*Контрольная работа*	Форма проверки и оценки усвоенных знаний, получения информации о характере познавательной деятельности, уровне самостоятельности и активности учащихся в учебном процессе, об эффективности методов, форм и способов учебной деятельности. Средство проверки умений	Перечень контрольных заданий	Критерии оценивания: 1. задания контрольной работы выполнены правильно и в полном объеме; 2. все этапы выполнения заданий достаточно пояснены; 3. работа оформлена аккуратно. Оценка: - «отлично» ставится, если выполнены все приведенные

		применять полученные знания, а так же средство контроля уровня выработки практических навыков решения задач по теме. Проводится в письменной форме.		требования, а так же продемонстрировано знание основных положений раздела, по которому проводится контрольная работа, владение терминологией и понятийным аппаратом, умение применять полученные знания к решению задач; - «хорошо» ставится, если при решении задач допущены неточности, работа выполнена неаккуратно, отсутствуют необходимые пояснения решения задач либо одно из заданий выполнено неверно; - «удовлетворительно» ставится, если правильно решены только половина заданий контрольной работы и (или) работа выполнена неаккуратно, отсутствуют необходимые пояснения решения задач, задания выполнены не в полном объеме. Если решено менее половины заданий контрольной работы, либо полностью отсутствует запись этапов решения задач (дан только ответ без пояснений), то за контрольную работу выставляется оценка «неудовлетворительно».
2.	Решение задач	Решение задач по указанной теме	Система стандартизированных заданий, предусмотренных на практическом занятии	- от 0 до 49,9 % выполненных заданий – не удовлетворительно; - от 50% до 69,9% - удовлетворительно; - от 70% до 89,9% - хорошо; - от 90% до 100% - отлично.
3.	Реферат	Средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной проблемы, самостоятельно проводить анализ этой проблемы с использованием аналитического инструментария	Темы к самостоятельной работе	Критерии оценки: 1) соответствие содержания письменной работы её теме, полнота раскрытия темы (оценка того, насколько содержание письменной работы соответствует заявленной теме и в какой мере тема раскрыта автором);

		соответствующей дисциплины, делать выводы, обобщающие авторскую позицию по поставленной проблеме		2) актуальность использованных источников (оценка того, насколько современны (по годам выпуска) источники, использованные при выполнении работы); 3) использование профессиональной терминологии (оценка того, в какой мере в работе отражены профессиональные термины и понятия, свойственные теме работы); 4) грамотность текста (оценка того, насколько владеет автор навыками письма в соответствии с грамматическими нормами языка. Проверка текста на наличие грамматических ошибок, употребление штампов, то есть избитых выражений; употребление слов-паразитов; ошибочное словообразование; ошибки в образовании словоформ; ошибки в пунктуации и т.п.); 5) наличие собственного отношения автора к рассматриваемой проблеме/теме (насколько точно и аргументировано выражено отношение автора к теме письменной работы): - от 0 до 49,9% выполненного задания - не зачтено; - 50% до 100% выполненного задания - зачтено
4.	Доклад / Презентация	подготовленное студентом самостоятельно публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной проблемы.	Темы к самостоятельной работе	Критерии оценки: - соответствие выступления теме, поставленным целям и задачам; - показал понимание темы, умение критического анализа информации; - продемонстрировал знание методов анализа и умение их применять; - обобщил информацию с помощью таблиц, схем, рисунков и т.д.; - сформулировал аргументи-

				рованные выводы; - оригинальность и креативность при подготовке презентации; - наличие собственного отношения автора к рассматриваемой проблеме/теме (насколько точно и аргументировано выражено отношение автора к теме доклада (презентации)): - от 0 до 49,9% выполненного задания - не зачтено; - 50% до 100% выполненного задания - зачтено
Оценочные средства для проведения промежуточной аттестации				
5.	*Зачет*	Контрольное мероприятие, которое проводится по окончании изучения дисциплины.	Вопросы к зачету	«*Зачтено*»: **знание** теории вопроса, понятийно-терминологического аппарата дисциплины (состав и содержание понятий, их связей между собой, их систему); **умение** анализировать проблему, содержательно и стилистически грамотно излагать суть вопроса; **владение** аналитическим способом изложения вопроса, навыками аргументации. «*Не зачтено*»*:* **знание** вопроса на уровне основных понятий; **умение** выделить главное, сформулировать выводы не продемонстрировано; **владение** навыками аргументации не продемонстрировано.

3. Типовые контрольные задания и/или иные материалы для проведения текущего контроля знаний, промежуточной аттестации, необходимые для оценки знаний, умений, навыков и/или опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Задания для проведения текущего контроля знаний

Тематика контрольных работ

1. Угрозы информационной безопасности организации и способы борьбы с ними
2. Современные средства защиты информации

3. Современные системы компьютерной безопасности
4. Современные средства противодействия экономическому шпионажу
5. Современные криптографические системы
6. Криптоанализ, современное состояние
7. Правовые основы защиты информации
8. Технические аспекты обеспечения защиты информации. Современное состояние
9. Атаки на систему безопасности и современные методы защиты
10. Современные пути решения проблемы информационной безопасности РФ

Примерный перечень заданий для контрольных работ

Теоретический вопрос на знание базовых понятий предметной области дисциплины, а также позволяющий оценить степень владения обучающимся принципами предметной области дисциплины, понимание их особенностей и взаимосвязи между ними.

1. Основные понятия информационной безопасности (ИБ).
2. Понятие тайны как объекта защиты ИБ.
3. Организация защиты информации (ЗИ).
4. Политика ИБ.
5. Основы нормативно-правовой ЗИ.
6. Основные нормативные документы РФ по ЗИ.
7. Защита государственной тайны.
8. Защита коммерческой тайны (КТ).
9. Доктрина ИБ РФ.
10. Организационная защита информации.
11. Работа с конфиденциальной информацией.
12. Функции службы безопасности.
13. Классификация способов защиты информации.
14. Основные действия по защите информации.
15. Основные принципы организации процесса защиты информации.
16. Угрозы информационной безопасности.
17. Средства защиты информации.
18. Классификация, возможности и назначение средств инженерно-техничекой защиты информации.
19. Физические средства защиты информации.
20. Аппаратные средства защиты информации.
21. Программные средства защиты информации.
22. Защита информации от утечки по техническим каналам.
23. Средства и способы защиты информации от утечки по визуально-оптическому и акустическому каналам.
24. Средства и способы защиты информации от утечки по электромагнитному и радио каналам.
25. Оценка эффективности системы ИБ.

Задания второго типа

Задание на анализ ситуации из предметной области дисциплины и выявление способности обучающегося выбирать и применять соответствующие принципы и методы решения практических проблем, близких к профессиональной деятельности.

1. Нарушение целостности данных, как правило, вызвано реализацией внешних или внутренних угроз? Обоснуйте ответ.
2. Нарушение конфиденциальности данных, как правило, вызвано реализацией внешних или внутренних угроз? Обоснуйте ответ.
3. Как соотносятся между собой понятия уязвимости и угроз? Обоснуйте ответ.
4. Как соотносятся между собой понятия угроз и рисков? Обоснуйте ответ.

5. В чем заключается отличие между разглашением и утечкой информации? Обоснуйте ответ.
6. Какими способами может быть реализовано противоправное преднамеренное овладение конфиденциальной информацией? Обоснуйте ответ.
7. Каким образом может происходить бесконтрольный выход конфиденциальной информации за пределы организации? Обоснуйте ответ.
8. В чем заключается отличие между служебной и профессиональной тайной? Обоснуйте ответ.
9. Что относится к информационным активам организации, и какие информационные активы являются наиболее ценным для организаций, осуществляющих различные виды деятельности (3-4 примера)? Обоснуйте ответ.
10. Какие сведения не могут составлять коммерческую тайну? Обоснуйте ответ.
11. Какие предъявляются требования к информации, составляющей коммерческую тайну? Обоснуйте ответ.
12. В чем заключается отличие между деятельностью ФСБ и ФСТЭК в сфере нормативно-правового регулирования защиты информации? Обоснуйте ответ.
13. В чем заключается отличие между правами собственности, владения и распоряжения информацией? Обоснуйте ответ.
14. Какая информация в соответствии с федеральными законами РФ ограничивается или запрещается к распространению? Обоснуйте ответ.
15. Какая информация в соответствии с федеральными законами РФ подлежит предоставлению или распространению? Обоснуйте ответ.
16. В чем заключается отличие между передачей и разглашением коммерческой тайны? Обоснуйте ответ.
17. В чем заключается отличие между предупреждением и выявлением угроз? Обоснуйте ответ.
18. В чем заключается отличие между выявлением и обнаружением угроз? Обоснуйте ответ.
19. Какие требования предъявляются к системе защиты информации? Обоснуйте ответ.
20. В чем заключается отличие между активными и пассивными средствами защиты информации? Обоснуйте ответ.
21. В чем заключается отличие между каналом передачи и каналом утечки информации? Обоснуйте ответ.
22. В чем заключается отличие между физическими и аппаратными средствами защиты информации? Обоснуйте ответ.
23. В чем заключается отличие между программными средствами собственной защиты и в составе вычислительной системы? Обоснуйте ответ.
24. Что легче: локализовать или обнаружить канал утечки информации? Обоснуйте ответ.
25. В чем заключается отличие между разовым и постоянным ресурсом, выделяемым на защиту информации? Обоснуйте ответ.

Задания для проведения промежуточной аттестации

Вопросы к зачету

1. Основные понятия и цели обеспечения информационной безопасности.
2. Правовая основа обеспечения информационной безопасности.
3. Основные положения Федерального закона «Об информации, информационных технологиях и о защите информации».
4. Основные положения Доктрины информационной безопасности Российской Федерации.
5. Понятие защиты информации и виды защищаемой информации.

6. Государственная политика обеспечения информационной безопасности (на примере иностранного государства).
7. Международные правовые акты в области защиты информации.
8. Специфика обеспечения информационной безопасности в правоохранительных органах.
9. Угрозы информационной безопасности в профессиональной сфере.
10. Задача обеспечения информационной безопасности, как составная часть борьбы с преступностью.
11. Виды каналов утечки информации.
12. Угрозы безопасности информации, обрабатываемой в автоматизированных системах.
13. Основные принципы и направления защиты автоматизированных систем от несанкционированного доступа.
14. Объективные факторы, представляющие угрозу безопасности информации.
15. Субъективные факторы, представляющие угрозу безопасности информации.
16. Методы ограничения доступа к информации, обрабатываемой в автоматизированных системах.
17. Уязвимости операционных систем и средства взлома паролей.
18. Виды и правовые источники конфиденциальной информации.
19. Способы защиты информации.
20. Классификация средств защиты информации.
21. Организационные меры по защите информации.
22. Технические мероприятия по защите информации.
23. Создание комплексной системы защиты информации на объекте информатизации.
24. Компьютерные сети, структура сети Интернет.
25. Протокол передачи данных TCP/IP (IP-адрес, доменное имя).
26. Сетевые службы (WWW, почта, FTP), пакеты, порты.
27. Организация доступа к сети Интернет.
28. Ресурсы общего доступа в сети, разграничение прав доступа.
29. Механизмы защиты от сетевых атак.
30. Понятие брандмауэр, правила файрвола.
31. Источники информации о сетевых атаках (журналы регистрации событий, сетевой трафик и т.п.).
32. Программные снифферы, анализаторы протоколов.
33. Методы определения IP-адреса абонента в сети Интернет.
34. Механизмы сокрытия пребывания абонента в сети Интернет.
35. Средства идентификации пользователей, контроль и разграничение прав.
36. Криптография как наука, симметричные и несимметричные алгоритмы шифрования.
37. Классификация методов шифрования информации.
38. Криптография и стеганография. Особенности и отличия.
39. Программные средства шифрации и защиты информации.
40. Понятие электронной подписи (ЭП), управление ключами.
41. Идентификация пользователя и аутентификация электронного сообщения.
42. Понятие вируса и троянской программы, средства защиты от разрушающих воздействий вредоносных программ.
43. Утилиты обслуживания компьютеров.

Схема соответствия типовых контрольных заданий и оцениваемых знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Код и наименование компетенции	Наименование индикатора достижения компетенции	Типовое контрольное задание
ПК-1 способен реализовывать образовательные программы в соответствии с требованиями федеральных государственных образовательных стандартов	ПК-1.1	Вопросы к зачету
	ПК-1.2	Задания первого и второго типа
	ПК-1.3	Задания для контрольных работ