Государственное бюджетное образовательное учреждение
высшего образования
«Башкирская академия государственной службы и управления при Главе Республики Башкортостан»

Кафедра государственного и муниципального управления

УТВЕРЖДАЮ

Ректор _____Д.М. Абдрахманов

"31" май 2023 г.

РАБОЧАЯ ПРОГРАММА

Информационная безопасность в государственном управлении

Б1.В.04

Уровень высшего образования

Магистратура

Направление подготовки

38.04.04. «Государственное и муниципальное управление»

Профиль
Цифровое государственное управление

Квалификация

Магистр

Форма обучения

заочная

Уфа 2023

Рабочая программа дисциплины «Б1.В.04
«Информационная безопасность в государственном управлении » / сост. Р.Х.Кунакбаев - Уфа: ГБОУ ВО «БАГСУ», 2023

Рабочая программа предназначена для обучающихся заочной форм обучения по направлению подготовки 38.04.04 «Государственное и муниципальное управление»

РЕКОМЕНДОВАНА заседанием кафедры государственного и муниципального управления
протокол №10 от "26" мая 2023 г.

Заведующий кафедрой
государственного и муниципального
управления И.Ш. Рысаев

Согласовано
Руководитель ОПОП Я.В.Ободец

Содержание

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

Целью освоения дисциплины «Информационная безопасность в государственном управлении» является формирование навыков организации и методологии обеспечения информацией органов государственного и муниципального управления; создание представления о функциях, структурах и штатах подразделения информационной безопасности; об организационных основах, принципах, методах и технологиях и управлении информационной безопасностью; развитие способностей по использованию существующей системы управления информацией.

Задачи:

Задачами освоения дисциплины «Информационная безопасность в государственном управлении » являются:

- получения студентами знаний по существующим угрозам безопасности информации, подбору и применению современных методов и способов защиты информации;
- формирование навыков, необходимых студентам по защите информации.

2 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код компетенции	Содержание компетенции (или её части)	Индикаторы компетенций	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
ПК-4	Способен анализировать процессы управления и осуществлять ее основные функции, организовать эффективную деятельность по реализации функций и полномочий государственных и муниципальных органов с учетом административных и технологических регламентов	**ИПК-4.1** Способен занимается научно-исследовательскими работами по проблемам государственного и муниципального управления **ИПК-4.2** Способен подготавливать обзоры и аналитические исследования по отдельным темам **ИПК-4.3** Способен организовывать научные исследования по вопросам, входящим в компетенцию подразделения с целью подготовки соответствующих научно обоснованных предложений, советов и рекомендаций	**Знать:** основные методы и средства получения информации; возможности использования информационных технологий в образовательной деятельности, включая требования к информационной безопасности. **Уметь**: получать необходимую информацию из различных типов источников с учетом информационной культуры; оформлять ссылки, сноски и библиографического списка

			для использования в профессиональной деятельности в сфере государственного и муниципального управления. **Владеть**: навыками для решения актуальных профессиональных задач на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; методами сбора и анализа данных с учетом информационной культуры

3 Структура и содержание дисциплины

3.1 Структура дисциплины

3.1.1 Заочная форма обучения

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 академических часов).

Вид работы	Трудоемкость, академических часов	
	4 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**10**	**10**
Лекции (Л)	6	6
Практические занятия (ПЗ)	4	4
Промежуточная аттестация (зачет с оценкой)	-	-
Самостоятельная работа:	**94**	**94**
- выполнение индивидуального творческого задания (ИТЗ): устный индивидуальный, групповой вопрос, тесты, типовые задачи для решения, творческие задания;	20	20
- самостоятельное изучение разделов;	20	20
- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий);	20	20
- подготовка к практическим занятиям;	20	20
- подготовка к рубежному контролю и т.п.	14	14
Вид итогового контроля	**4 зачет**	**4 зачет**

Разделы дисциплины, изучаемые в 4 семестре

№ раздела	Наименование разделов	Количество часов			
		всего	аудиторная работа		внеауд. работа
			Л	ПЗ	
1	Понятие информационной безопасности. Основные составляющие	36	2	2	32
2	Законодательный уровень информационной безопасности. Административный уровень информационной безопасности	36	2	-	34
3	Объектно-ориентированный подход к рассмотрению защищаемых систем. Наиболее распространенные угрозы информационной безопасности и еѐ составляющие	36	2	2	32
	Итого:	108	6	4	98

Практические занятия

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Понятие информационной безопасности. Основные составляющие	2
2	2	Законодательный уровень информационной безопасности. Административный уровень информационной безопасности	1
3	3	Объектно-ориентированный подход к рассмотрению защищаемых систем. Наиболее распространенные угрозы информационной безопасности и еѐ составляющие	1
		Итого:	4

3.2 Содержание разделов дисциплины

№ раздела	Наименование раздела	Содержание раздела
1	Понятие информационной безопасности. Основные составляющие	Информационная безопасность. Защита информации, субъект информационных отношений, неприемлемый ущерб. Доступность, целостность, конфиденциальность. Компьютерное преступление, жизненный цикл информационных систем
2	Законодательный уровень информационной безопасности. Административный уровень информационной безопасности	Российское законодательство в области информационной безопасности. Зарубежное законодательство в области информационной безопасности. Стандарты и спецификации в области информационной безопасности. Основные понятия административного уровня, политика безопасности. Жизненный цикл информационной системы. Синхронизация программы безопасности с жизненным циклом систем. Управление рисками
3	Объектно-ориентированный подход к	Сложные системы. Структурный подход. Объектноориентированный подход, класс, объект, метод объекта, инкапсу-

	рассмотрению защищаемых систем. Наиболее распространенные угрозы информационной безопасности и еѐ составляющие	ляция, наследование, полиморфизм, грань объекта, уровень детализации ИС, деление на субъекты и объекты, безопасность повторного использования объектов, учет семантики. Операционная система как сервис безопасности. Основные определения и критерии классификации угроз. Угроза, атака, уязвимость, окно опасности, источник угрозы, злоумышленник. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности.

3.3Курсовой проект (курсовая работа) – не предусмотрена

4.Учебно-методическое обеспечение дисциплины

4.1.Основная литература

1. Фомин Д.В. Информационная безопасность [Электронный ресурс]: учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения/ Фомин Д.В.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2018.— 54 с.— Режим доступа: http://www.iprbookshop.ru/77320.html

2. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 256 с.— Режим доступа: http://www.iprbookshop.ru/33430.html

3. Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс]/ Фаронов А.Е.— Электрон. текстовые данные.— М.: ИнтернетУниверситет Информационных Технологий (ИНТУИТ), 2016.— 154 с.— Режим доступа: http://www.iprbookshop.ru/52160.html

4.2.Дополнительная литература

1. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ Галатенко В.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 с.— Режим доступа: http://www.iprbookshop.ru/52209.html

2. Авдошин С.М. Технологии и продукты Microsoft в обеспечении информационной безопасности [Электронный ресурс]/ Авдошин С.М., Савельева А.А., Сердюк В.А.— Электрон. текстовые данные.— Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017.— 412 с.— Режим доступа: http://www.iprbookshop.ru/72341.html

3. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 с.— Режим доступа: http://www.iprbookshop.ru/10677.html

4.3 Периодические издания

- Научная электронная библиотека eLIBRARY.RU. Режим доступа: https://elibrary.ru
- Российская Государственная Библиотека. Режим доступа: https://www.rsl.ru
- Международная реферативная база данных научных изданий Springerlink Режим доступа: https://link.springer.com
- Цифровой образовательный ресурс IPR SMART Режим доступа: https://iprbookshop.ru

4.4 Интернет-ресурсы

- Справочно-правовая система Консультант Плюс - http://www.consultant.ru
- Справочно-правовая система Гарант – http://www.garant.ru
- Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru
- «Национальная платформа открытого образования» https://openedu.ru

4.5 Методические указания к практическим занятиям (семинарам)

Для подготовки к практическим занятиям необходимо ознакомиться с планом занятий, изучить конспект лекций, рекомендованную литературу, самостоятельно проверить знания по теме.

Практические занятия проходят в учебных группах по всем темам курса. Основные методы, используемые в ходе проведения практических занятий по дисциплине «Информационная безопасность в государственном управлении» - это методы опроса, докладов, дискуссий, творческих работ с последующим их обсуждением и анализом допускаемых ошибок. При ответе на вопросы необходимо внимательно прочитать их текст и попытаться дать аргументированное объяснение. Порядок ответа на вопрос может быть различным: либо вначале делается вывод, а затем приводятся аргументы в его защиту, либо дается развернутая аргументация решения, на основании которой предлагается ответ.

При сомнении в правильности ответа, можно посоветоваться с другими обучающимися или обратиться за консультацией к преподавателю.

Занятия проводятся в форме свободной дискуссии при активном участии всех обучающихся, у которых всегда имеется возможность дополнить выступающих, не соглашаться с ними, высказывать альтернативные точки зрения и отстаивать их, поправлять выступающих, задавать им вопросы, предлагать для обсуждения новые проблемы. Вопросы могут быть заданы и преподавателю.

Обсуждение каждого вопроса, упражнения, задачи (ситуации) обычно заканчиваются кратким заключением преподавателя. По окончании занятия преподаватель подводит итоги дискуссии и высказывает свою точку зрения, отмечая положительные или отрицательные моменты.

4.6 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

В образовательном процессе применяются аудитории 205, 310.

Аудитория 310.

Приложение: Microsoft Office 2010 Standart (договор поставки программного обеспечения № 178-ПО/2010 от 30.11.2010 г. (ООО "Абсолют-Информ"). Кол-во лицензий: 55 шт.)

Microsoft Office Professional Plus 2007 (договор поставки программного обеспечения № 007-ПО/2009 от 24.11.2009 г. (ООО "Абсолют-Информ"). Кол-во лицензий: 37 шт.)

Учебные программы:

- Деловая игра "Бизнес-курс. Максимум. Фирма" (договор № 110622/1 от 22.06.2011 г. на предоставление неисключительных (пользовательских) прав на программу для ЭВМ (ООО "Высшие компьютерные курсы бизнеса"). Кол-во лицензий: 10 шт.)

- Microsoft Vizio Standart 2007 (договор поставки программного обеспечения № 028 – ПО/2009 от 10.12.2009 г (ООО "Аир-Информ"). Кол-во лицензий: 12 шт.)

- СПС "Консультант Плюс" (соглашение об информационной поддержке от 09.06.2016 г. (ООО Компания права "Респект", РИЦ 33. Кол-во лицензий: сетевая версия (неограниченно))

- СДО "Прометей" (лицензия на право использования ПО по договору поставки программного обеспечения № 1/БАГСУ/02/07 от 14.03.2007 г. (ООО "Виртуальные технологии в образовании"). Кол-во лицензий: сетевая версия (неограниченно)).

5 Материально-техническое обеспечение дисциплины

Лекционные и практические занятия будут проходить в специализированных аудиториях, которые оборудованы необходимым информационным обеспечением.

Аудитория 205.

Доска – классная -1 шт.

Доска белая магнитная М007100281 - 1 шт.

Герб РФ и РБ.

Флаги РФ и РБ.

Слова гимна РФ и РБ.

Трибуна настольная - 1 шт.

56 посадочных мест.

Аудитория 310.

Персональный компьютер – 13 шт. с выходом в Интернет.

Доска маркерно-магнитная TZ 7484- 1 шт.

Доска классная -1 шт.

29 посадочных мест.

К рабочей программе прилагаются:

- Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине (модулю), который разрабатывается в виде отдельного документа;
- Методические указания для обучающихся по освоению дисциплины

Приложение

Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины включает в себя лекционные и практические занятия и самостоятельную работу обучающихся.

Лекционные занятия предназначены для теоретического осмысления и обобщения сложных разделов курса.

На практических занятиях предполагается рассмотрение теоретических парадигм и анализ конкретных практических вопросов в рамках изучаемой дисциплины. Обучающимся будут предложены задания, которые нацелены на выработку навыка аналитического мышления, аргументированного изложения своей точки зрения, способности вести диалог с участниками дискуссий.

Учебные занятия проводятся в форме контактной работы (аудиторной и внеаудиторной) и самостоятельной работы обучающихся.

Работа с рекомендованной литературой. При работе с основной и дополнительной литературой целесообразно придерживаться такой последовательности. Сначала прочитать весь заданный текст в быстром темпе. Цель такого чтения заключается в том, чтобы создать общее представление об изучаемом материале, понять общий смысл прочитанного. Затем прочитать вторично, более медленно, чтобы в ходе чтения понять и запомнить смысл каждой фразы, каждого положения и вопроса в целом. Чтение приносит пользу и становится продуктивным, когда сопровождается записями. Это может быть составление плана прочитанного текста, тезисы или выписки, конспектирование и др. Выбор вида записи зависит от характера изучаемого материала и целей работы с ним. Если материал содержит новую и трудно усваиваемую информацию, целесообразно его законспектировать. План – это схема прочитанного материала, перечень вопросов, отражающих структуру и последовательность материала.

Подготовка к практическим занятиям. Для успешного освоения материала обучающимся рекомендуется сначала ознакомиться с учебным материалом, изложенным в лекциях и основной литературе, затем выполнить самостоятельные задания, при необходимости обращаясь к дополнительной литературе. Необходимо помнить, что на лекции обычно рассматривается не весь материал, а только его наиболее важная и сложная часть, требующая пояснений преподавателя в процессе контактной работы с обучающимися. Остальная его часть восполняется в ходе самостоятельной работы. В связи с этим работа с рекомендованной литературой обязательна. В процессе этой работы обучающийся должен стремиться понять и запомнить основные положения рассматриваемого материала, примеры, поясняющие его, разобраться в иллюстративном материале. Заканчивать подготовку следует составлением плана

(перечня основных пунктов) по изучаемому материалу (вопросу). Такой план позволяет составить концентрированное, сжатое представление по изучаемым вопросам и структурировать изученный материал. Целесообразно готовиться к практическим занятиям за 1-2 недели до их начала.

Выполнение заданий нацелено на выработку навыка аналитического мышления, аргументированного изложения своей точки зрения, способности вести диалог с участниками дискуссий. Выполнение заданий позволяет оценивать и диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения.

Подготовка к экзамену (зачету, зачету с оценкой). При подготовке к экзамену (зачету, зачету с оценкой) необходимо ориентироваться на конспекты лекций, рабочую программу дисциплины, фонд оценочных средств, нормативную, учебную и рекомендуемую литературу. Подготовка обучающегося к экзамену (зачету, зачету с оценкой) включает в себя три этапа: самостоятельная работа в течение семестра; непосредственная подготовка по темам курса; подготовка к ответу на вопросы.

Государственное бюджетное образовательное учреждение
высшего образования
«Башкирская академия государственной службы и управления при Главе Республики Башкортостан»

Кафедра государственного и муниципального управления

Фонд оценочных средств

по дисциплине
Б1.В.04 «Информационная безопасность в государственном управлении»

Уровень высшего образования
Магистратура

Направление подготовки
38.04.04. «Государственное и муниципальное управление»

Профиль
Цифровое государственное управление

Квалификация
Магистр

Форма обучения
заочная

Уфа 2023

Фонд оценочных средств предназначен для контроля знаний обучающихся заочной форм обучения по направлению подготовки 38.04.04 «Государственное и муниципальное управление» по дисциплине Б1.В.04 «Информационная безопасность в государственном управлении»

Составитель: Р.Х.Кунакбаев

Фонд оценочных средств является приложением к рабочей программе по дисциплине Б1.В.04 «Информационная безопасность в государственном управлении»

Паспорт фонда оценочных средств
по дисциплине «Информационная безопасность в государственном управлении»

1. Основные сведения о дисциплине

4.1.1 Заочная форма обучения

Общая трудоемкость дисциплины составляет 4 зачетные единицы (108 академических часа).

Вид работы	Трудоемкость, академических часов	
	4 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**10**	**10**
Лекции (Л)	6	6
Практические занятия (ПЗ)	4	4
Промежуточная аттестация (зачет с оценкой)	-	-
Самостоятельная работа:	**94**	**94**
- выполнение индивидуального творческого задания (ИТЗ): устный индивидуальный, групповой вопрос, тесты, типовые задачи для решения, творческие задания;	20	20
- самостоятельное изучение разделов;	20	20
- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий);	20	20
- подготовка к практическим занятиям;	20	20
- подготовка к рубежному контролю и т.п.	14	14
Вид итогового контроля	**4 зачет**	**4 зачет**

Разделы дисциплины, изучаемые в 4 семестре

№ раздела	Наименование разделов	Количество часов			
		всего	аудиторная работа		внеауд. работа
			Л	ПЗ	
1	Понятие информационной безопасности. Основные составляющие	36	2	2	32
2	Законодательный уровень информационной безопасности. Административный уровень информационной безопасности	36	2	-	34
3	Объектно-ориентированный подход к рассмотрению защищаемых систем. Наиболее распространенные угрозы информационной безопасности и еѐ составляющие	36	2	2	32
	Итого:	108	6	4	98

Практические занятия

№ занятия	№ раздела	Тема	Кол-во часов
1	1	Понятие информационной безопасности. Основные составляющие	2
2	2	Законодательный уровень информационной безопасности. Административный уровень информационной безопасности	1
3	3	Объектно-ориентированный подход к рассмотрению защищаемых систем. Наиболее распространенные угрозы информационной безопасности и еѐ составляющие	1
		Итого:	4

2 Требования к результатам обучения по дисциплине, формы их контроля и виды оценочных средств

Процесс изучения дисциплины направлен на формирование следующих результатов обучения:

Формируемые компетенции	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Типы контроля*
ПК-4Способен анализировать процессы управления и осуществлять ее основные функции, организовать эффективную деятельность по реализации функций и полномочий государственных и муниципальных органов с учетом административных и технологических регламентов	**Знать:** основные методы и средства получения информации; возможности использования информационных технологий в образовательной деятельности, включая требования к информационной безопасности.	Тестирование по лекционному материалу. Письменные контрольные работы. Устное индивидуальное собеседование и опрос на практических и семинарских занятиях (см. п.4 Вопросы для самопроверки обучающихся**)** Зачет
	Уметь: получать необходимую информацию из различных типов источников с учетом информационной культуры; оформлять ссылки, сноски и библиографического списка для использования в профессиональной деятельности в сфере государственного и муниципального управления	Письменные и устные работы на решение типовых задач. Устное индивидуальное собеседование Подготовка к докладам Зачет

Формируемые компетенции	*Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций*	*Типы контроля*
	Владеть: навыками для решения актуальных профессиональных задач на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; методами сбора и анализа данных с учетом информационной культуры	Выполнение индивидуального творческого задания. Зачет

3 Организация и учебно-методическое обеспечение самостоятельной работы обучающихся

Самостоятельная работа обучающихся (СРО) направлена на закрепление и углубление освоенного учебного материала, развитие практических умений и навыков.

Виды СРО:

Изучение литературы в соответствии с темами рабочей программы, конспектирование текстов для подготовки выступлений на семинарских занятиях; работа со словарями и справочниками по уточнению ключевых понятий изучаемой темы; ознакомление с нормативными документами в соответствии с задачами рассматриваемой темы занятия.

Составление плана и тезисов ответа на семинарских занятиях; подготовка сообщений к выступлению на семинаре.

Решение типовых и творческих заданий.

Подготовка к рубежному контролю и т.п.

Темы для самостоятельного изучения:

1. Законодательная база Российской Федерации по обеспечению информационной безопасности.
2. Международные нормативно-правовые акты в области информационной безопасности.
3. Современная постановка задачи защиты информации.
4. Методологический базис решения задач защиты информации.
5. Система стандартизации в области защиты информации.
6. Моделирование процессов защиты информации.
7. Понятие угрозы безопасности информации. Риски и управление рисками
8. Системная классификация угроз безопасности информации.

9. Методы оценки уязвимости информации. Формула оценки уязвимости информации.

10. Методы оценки достоверности информации.

11. Методы оценки ущерба от реализации угроз безопасности информации.

12. Способы несанкционированного доступа к данным. Методы обеспечения недоступности данных.

13. Анализ методик определения требований к защите информации.

14. Параметры защищаемой информации.

15. Принципы защиты информации от несанкционированного доступа.

Домашние задания:

– чтение текста (учебника, первоисточника, дополнительной литературы), конспектирование текста;

– ознакомление с нормативными документами;

– повторная работа над учебным материалом (учебника, первоисточника, дополнительной литературы);

– составление плана и тезисов ответа; изучение нормативных материалов;

– подготовка сообщений к выступлению на семинаре.

Работа в системе дистанционного обучения БАГСУ. При необходимости обучающийся может получить логин и пароль для работы в системе дистанционного обучения БАГСУ. В этом случае обеспечивается доступ к электронным курсам «Информационная безопасность в государственном управлении». Электронные курсы включают тексты лекций, мультимедийные презентации, тесты и контрольные задания.

Устный индивидуальный опрос

Устный индивидуальный опрос проводится после изучения каждой новой темы с целью выяснения наиболее сложных вопросов, степени усвоения информации.

Обучающийся излагает содержание вопроса изученной темы.

Критерии и методика оценивания:

- 5 баллов выставляется обучающемуся, если точно используется терминология, показано уверенное владение нормативной базой;

- 4 балла выставляется обучающемуся, допущены один-два недочета при освещении основного содержания ответа, нет определенной логической последовательности, не в полной мере точно используется терминология;

- 3 балла выставляется обучающемуся, нет общего понимания вопроса, имеются затруднения или допущены ошибки в определении понятий, использовании терминологии.

Устный групповой опрос

Устный групповой опрос проводится после изучения каждой новой темы с целью выяснения наиболее сложных вопросов, степени усвоения информации, поддержания внимания слушающей аудитории.

Критерии и методика оценивания:

- 5 баллов выставляется обучающемуся, если точно используется терминология, показано уверенное владение нормативной базой;

- 4 балла выставляется обучающемуся, допущены один-два недочета при освещении основного содержания ответа, нет определенной логической последовательности, неточно используется терминология;

- 3 балла выставляется обучающемуся, нет общего понимания вопроса, имеются затруднения или допущены ошибки в определении понятий, использовании терминологии.

Вопросы для самопроверки обучающихся

Вопросы для самопроверки при подготовке к зачету (36 вопросов):

1. Информационная безопасность. Защита информации, субъект информационных отношений, неприемлемый ущерб.
2. Доступность, целостность, конфиденциальность. Компьютерное преступление, жизненный цикл информационных систем.
3. Сложные системы. Структурный подход.
4. Основные определения и критерии классификации угроз.
5. Угроза, атака, уязвимость, окно опасности, источник угрозы, злоумышленник.
6. Основные угрозы доступности. Основные угрозы целостности. Основные угрозы конфиденциальности.
7. Российское законодательство в области информационной безопасности.
8. Зарубежное законодательство в области информационной безопасности.
9. Стандарты и спецификации в области информационной безопасности.
10. Основные понятия, политика безопасности.
11. Жизненный цикл информационной системы.
12. Синхронизация программы безопасности с жизненным циклом систем. Управление рисками.
13. Основные классы мер процедурного уровня.
14. Управление персоналом. Физическая защита.
15. Поддержание работоспособности.
16. Реагирование на нарушения режима безопасности.
17. Планирование восстановительных работ.
18. Основные понятия программно-технического уровня. Архитектурная безопасность.
19. Экранирование. Анализ защищѐнности.
20. Отказоустойчивость. Безопасное восстановление.
21. Основные понятия криптографии.
22. Парольная аутентификация. Одноразовые пароли. Сервер аутентификации Kerberos.
23. Идентификация/аутентификация с помощью биометрических данных.

24. Управление доступом. Ролевое управление доступом.
25. Активный аудит. Шифрование.
26. Симметричный метод шифрования.
27. Асимметричный метод шифрования.
28. Секретный и открытый ключ.
29. Криптография. Контроль целостности
30. Цифровые сертификаты.
31. Электронная цифровая подпись.
32. Экранирование. Фильтрация. Межсетевые экраны.
33. Классификация межсетевых экранов.
34. Архитектурная безопасность.
35. Транспортное экранирование. Анализ защищенности.
36. Сетевой сканер. Антивирусная защита.

5. Учебно-методическое обеспечение дисциплины

5.1.Основная литература

1. Фомин Д.В. Информационная безопасность [Электронный ресурс]: учебно-методическое пособие по дисциплине «Информационная безопасность» для студентов экономических специальностей заочной формы обучения/ Фомин Д.В.— Электрон. текстовые данные.— Саратов: Вузовское образование, 2018.— 54 c.— Режим доступа: http://www.iprbookshop.ru/77320.html

2. Артемов А.В. Информационная безопасность [Электронный ресурс]: курс лекций/ Артемов А.В.— Электрон. текстовые данные.— Орел: Межрегиональная Академия безопасности и выживания (МАБИВ), 2014.— 256 c.— Режим доступа: http://www.iprbookshop.ru/33430.html

3. Фаронов А.Е. Основы информационной безопасности при работе на компьютере [Электронный ресурс]/ Фаронов А.Е.— Электрон. текстовые данные.— М.: ИнтернетУниверситет Информационных Технологий (ИНТУИТ), 2016.— 154 c.— Режим доступа: http://www.iprbookshop.ru/52160.html

5.2.Дополнительная литература

1. Галатенко В.А. Основы информационной безопасности [Электронный ресурс]/ Галатенко В.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 c.— Режим доступа: http://www.iprbookshop.ru/52209.html

2. Авдошин С.М. Технологии и продукты Microsoft в обеспечении информационной безопасности [Электронный ресурс]/ Авдошин С.М., Савельева А.А., Сердюк В.А.— Электрон. текстовые данные.— Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017.— 412 c.— Режим доступа: http://www.iprbookshop.ru/72341.html

3. Башлы П.Н. Информационная безопасность и защита информации [Электронный ресурс]: учебное пособие/ Башлы П.Н., Бабаш А.В., Баранова

Е.К.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2012.— 311 c.— Режим доступа: http://www.iprbookshop.ru/10677.html

5.3 Периодические издания

- Научная электронная библиотека eLIBRARY.RU. Режим доступа: https://elibrary.ru
- Российская Государственная Библиотека. Режим доступа: https://www.rsl.ru
- Международная реферативная база данных научных изданий Springerlink Режим доступа: https://link.springer.com
- Цифровой образовательный ресурс IPR SMART Режим доступа: https://iprbookshop.ru

5.4 Интернет-ресурсы

- Справочно-правовая система Консультант Плюс - http://www.consultant.ru
- Справочно-правовая система Гарант – http://www.garant.ru
- Информационная система "Единое окно доступа к образовательным ресурсам" http://window.edu.ru
- «Национальная платформа открытого образования» https://openedu.ru

6 Оценочные средства для проверки освоения изученных компетенций

6.1. ПК-4 Способен анализировать процессы управления и осуществлять ее основные функции, организовать эффективную деятельность по реализации функций и полномочий государственных и муниципальных органов с учетом административных и технологических регламентов

Фонд тестовых заданий по дисциплине:

1.Цифровая информация это?

1. информация, хранение, передача и обработка которой осуществляется средствами ИКТ
2. информация, хранение, передача и обработка которой осуществляется средствами почты
3. информация, хранение, передача и обработка которой осуществляется средствами радиосвязи

2 Защита информации это?

1. деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию
2. деятельность по передачи защищаемой информации, другим лицам
3. деятельность по предотвращению нанесению ущерба гражданам РФ от незаконных действий коллекторов и прочих организаций

3. Основные виды угроз для цифровой информации?
1. Кража информации
2. Утечка информации
3. Разрушение информации
4. Уничтожение информации
5. Защита информации
6. Резервирование информации
7. Архивирование информации

4. Установите соответствие природе возникновения информационных угроз:
А) естественные угрозы
Б) искусственные угрозы
Варианты ответов
1. вызванные воздействиями на КС объективных физических процессов или стихийных природных явлений
2. вызванные деятельностью человека

5. Установите соответствие источнику угрозы информации:
А) природная среда
Б) человек
В) санкционированные программно-аппаратные средства
Г) несанкционированные программно-аппаратные средства
Варианты ответов
1. например, стихийные бедствия
2. например, разглашение конфиденциальных данных
3. например, отказ в работе операционной системы
4. например, заражение компьютера вирусами

6 По степени воздействия различают следующие угрозы информации:
1. пассивные угрозы
2. активные угрозы
3. радиоактивные угрозы
4. химические угрозы

7. Установите соответствие типу угроз:
А) пассивные угрозы
Б) активные угрозы
Варианты ответов
1. которые при реализации ничего не меняют в структуре и содержании КС (угроза копирования данных)
2. которые при воздействии вносят изменения в структуру и содержание КС (внедрение аппаратных и программных спецвложений)

8. Несанкционированное воздействие на информацию это?

1. преднамеренная порча или уничтожение информации, а также информационного оборудования со стороны лиц, не имеющих на это права (санкции)

2. Происходит вследствие ошибок пользователя, а также из-за сбоев в работе оборудования или программного обеспечения

9. Непреднамеренное воздействие на информацию это?

1. преднамеренная порча или уничтожение информации, а также информационного оборудования со стороны лиц, не имеющих на это права (санкции)

2. Происходит вследствие ошибок пользователя, а также из-за сбоев в работе оборудования или программного обеспечения

10 Перечислите пример несанкционированное воздействия на информацию?

1. создание компьютерных вирусов
2. хакерские атаки
3. потеря носителя с информацией
4. случайное удаление информации

Комплект разноуровневых практических заданий

Для самостоятельного освоения и / или расширения знаний, умений, владений предусмотрены несколько уровней практических заданий:

- базовый,
- повышенный,
- творческий.

Типовые задания базового уровня

Задание 1.

Подготовьте мини-глоссарий и дайте определение следующим понятиям:

собственник информации,
владелец информации,
пользователь, распоряжение,
дезинформация,
информационная безопасность,
защита информации,
угроза,
атака,
злоумышленник,
политика безопасности,
конфиденциальность информации,
целостность информации,
доступность информации,
идентификатор,
пароль,
ключ,
учетная запись пользователя,

идентификация,
аутентификация,
отказ от обслуживания,
утечка,
разглашение.

Критерии оценки заданий базового уровня

Показатель оценки	Распределение баллов
Точность воспроизведения учебного материала (терминов, правил, фактов, описаний и т.д.)	1
Точность различения и выделения изученных материалов	1
Максимальный балл	2

Типовые задания повышенного уровня

Задание 1.

Сравнить способы учета электронных конфиденциальных документов, передаваемых по линии защищенной компьютерной связи, выявить критерии определения эффективности каждого из способов

Задание 2

Составить схему каналов возможной утраты конфиденциальной информации, находящейся в компьютере, локальной сети проанализировать степень опасности каждого канала

Типовые задания творческого уровня

Задание 1.

Графически (схематически) описать технологию выполнения процедур и операций конкретной части того или иного элемента системы защиты информации (по выбору преподавателя).

Задание 2.

Желая помочь своим коллегам, программист Сальников и адвокат Сабуров - работники нотариальной конторы «ОКС» - внесли изменения в программу «Акты и документы о недвижимости». В результате этих действий была уничтожена информация, касающаяся опыта работы конторы в области регистрации недвижимости за последний год и нарушена работа ПК. Руководитель нотариальной конторы обратился к прокурору с заявлением о возбуждении уголовного дела против Сальникова и Сабурова. Есть ли в действиях Сальникова и Сабурова состав преступления?

Критерии оценки заданий творческого уровня

Показатель оценки	Распределение баллов
Способность к поиску и систематизации информации в профессиональной сфере	1

Способность синтезировать новую информацию на основе имеющихся данных	1
Наличие обоснованных выводов на основе интерпретации информации	1
Установление причинно-следственных связей, выявление закономерностей	1
Максимальный балл	4

Примерные темы докладов

1. Понятие, проблемы и структура информационной безопасности (на примере фирм различных типов).
2. Классификация информационных ресурсов ограниченного доступа к ним персонала фирмы, характеристика каждой группы.
3. Информационная безопасность, история формирования.
4. Концепция информационной безопасности.
5. Основы экономической безопасности предпринимательской деятельности.
6. Анализ законодательных актов о защите информационных ресурсов ограниченного доступа.
7. Информационная безопасность (по материалам зарубежных источников и литературы).
8. Правовые основы защиты конфиденциальной информации.
9. Экономические основы защиты конфиденциальной информации.
10. Организационные основы защиты конфиденциальной информации.
11. Структура, содержание и методика составления перечня сведений, составляющих предпринимательскую тайну.
12. Построение и функционирование защищенного документооборота.
13. Анализ инструкции по обработке и хранению конфиденциальных документов.
14. Направления и методы защиты документов на бумажных носителях.
15. Направления и методы защиты машиночитаемых документов.
16. Направления и методы защиты электронных документов.
17. Архивное хранение конфиденциальных документов.
18. Направления и методы защиты аудио и визуальных документов.
19. Виды и назначение технических средств защиты информации в помещениях, используемых для ведения переговоров и совещаний.
20. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.
21. Соотношение источников, каналов распространения и каналов утечки информации.
22. Анализ опыта защиты информации в зарубежных странах.
23. Анализ конкретной автоматизированной системы, предназначенной для обработки и хранения информации о конфиденциальных документах фирмы.

24. Основы технологии обработки и хранения конфиденциальных документов.

25. Назначение, виды, структура и технология функционирования системы защиты информации.

26. Направления экономического анализа системы защиты информации.

27. Поведение персонала и охрана фирмы в экстремальных ситуациях различных типов.

28. Направления и методы защиты профессиональной тайны.

29. Направления и методы защиты служебной тайны.

30. Направления и методы защиты персональных данных о гражданах.

31. Методы защиты личной и семейной тайны.

32. Проблемы управления персоналом и защиты информации в предпринимательской деятельности.

33. Порядок подбора персонала для работы с конфиденциальной информацией.

34. Тестирование и проведение собеседования с претендентами на должность, связанную с секретами фирмы.

35. Назначение, структура и методика построения разрешительной системы доступа персонала к секретам фирмы.

36. Порядок подготовки и проведения переговоров и совещаний по конфиденциальным вопросам.

Критерии оценки доклада

Соответствие содержания доклада заявленной теме, поставленным целям и задачам	0,5
Логичность и последовательность в изложении материала	0,5
Привлечение актуальных нормативных актов и современной научной литературы	1
Степень обоснованности аргументов и обобщений (полнота, глубина, всесторонность раскрытия темы, корректность аргументации и системы доказательств, характер и достоверность примеров, наличие знаний интегрированного характера, способность к обобщению)	1
Самостоятельность изучения и анализа материала	1
Речевая культура (научный стиль изложения, владение понятийным аппаратом, четкость, лаконичность)	1
Использование демонстрационных материалов (наличие и качество презентации)	1
ИТОГО	6

Количество контрольно-измерительных материалов

№ п/п	Контролируемые компетенции	Контрольно-измерительные материалы, количество заданий или вариантов				
		Тестовые задания	*Типовые задачи/базовые*	*Типовые задачи\повышенные*	*Творческие задания*	*Доклады*

1	ПК-4	10	1	2	2	36
	Всего:	10	1	2	2	36

Ключи к тестовым задания

1	1	**6**	1,2
2	1	**7**	А)–1 Б)-2
3	1,2,3,1	**8**	1
4	А)–1 Б)-2	**9**	2
5	А)–1 Б)–2 В)-3 Г)-4	**10**	1,2