Образовательное частное учреждение высшего образования
«ГУМАНИТАРНО-СОЦИАЛЬНЫЙ ИНСТИТУТ»

УТВЕРЖДЕНО
заседанием Ученого совета
протокол №7 от 27.06.2023 г.
приказ ректора об утв. ОПВО
№ 01-03/70 П от 28.06.2023 г.
Ректор _____ Л.Ф. Логинова

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.31 «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Код и направление подготовки:

38.03.05 «Бизнес-информатика»

Направленность (профиль):
«**Информационная бизнес-аналитика**»

Красково - 2023

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта высшего образования (далее – ФГОС ВО) по программе подготовки 38.03.05 «Бизнес-информатика».

Организация – разработчик: Образовательное частное учреждение высшего образования «Гуманитарно-социальный институт».

Разработчики:

к.т.н., доц.		Габан А.В.
ученая степень, звание	*подпись*	*ФИО*
ученая степень, звание	*подпись*	*ФИО*

Рабочая программа учебной дисциплины утверждена на заседании кафедры «Общеобразовательных дисциплин» от 22.06.2023 г. протокол № 10

Заведующий кафедрой
Д.ф.н., профессор _____ Кузнецова Т.Ф.
подпись

Наименование дисциплины – Информационная безопасность

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

Цель освоения дисциплины заключается в формировании у студентов, обучающихся по направлению подготовки 38.03.05 Бизнес-информатика, навыков в области информационной безопасности. Применение методов управления и использования технологий, обеспечивающих информационную безопасность, и определяет следующие **задачи:** формирование знаний в области обеспечения информационной безопасности; изучение основных технологий, обеспечивающих информационную безопасность; приобретение студентами практических навыков управления информационной безопасностью.

Дисциплина «Информационная безопасность» в рамках воспитательной работы направлена на формирование у обучающихся; психологической готовности к профессиональной деятельности по избранной профессии; воспитание у обучающихся уважения к труду, людям труда, трудовым достижениям и подвигам; формирование у обучающихся потребности трудиться, добросовестного, ответственного и творческого отношения к разным видам трудовой деятельности; развитие навыков высокой работоспособности и самоорганизации, гибкости, умение действовать самостоятельно, активно и ответственно, мобилизуя необходимые ресурсы, правильно оценивая смысл и последствия своих действий; коммуникативной культуры и развитие органов студенческого самоуправления; исследовательского и критического мышления у обучающихся; повышение мотивации к научно- исследовательской деятельности, интереса к науке в целом; развитие творческой культуры и эрудиции; навыков творческого применения на практике достижений научного прогресса; развитие навыков решения прикладных задач с использованием научных методов, продвижение собственных научных идей.

Планируемые результаты обучения

Процесс освоения дисциплины направлен на формирование следующих компетенций:
ОПК-3 Способен управлять процессами создания и использования продуктов и услуг в сфере информационно-коммуникационных технологий, в том числе разрабатывать алгоритмы и программы для их практической реализации;
ПК-2 Способен выполнять работы по созданию (модификации) и сопровождению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы.
Подготовка по дисциплине реализуется на основе профессионального стандарта: ПС 06.015 «Специалист по информационным системам».

Матрица связи дисциплины Б1.О.31 «Информационная безопасность» и компетенций, формируемых на основе изучения дисциплины, с временными этапами освоения ее содержания

Код и наименование компетенции выпускника	**Код и наименование индикатора компетенции выпускника**	**Код индикатора компетенции выпускника**	**Код и наименование дескрипторов (планируемых результатов обучения выпускников)**
ОПК-3 Способен управлять процессами создания и использования продуктов и услуг в сфере информационно-коммуникационных технологий, в том числе разрабатывать алгоритмы и программы для их практической реализации	**ОПК-3.2.** Принимает решения относительно выбора методов и технологий управления процессами организации, в том числе на основе норм права, и оценивает их последствия	**ОПК-3.2.**	**ОПК-3.2.1** ***Знать:*** базовые теоретические положения в области информационной безопасности; основы информационной безопасности в категориальной сетке законодательного, административного и процедурного уровня; методы и средства решения задач профессиональной деятельности с учетом основных требований информационной безопасности; **ОПК-3.2.2** ***Уметь:*** использовать базовые теоретические положения дисциплины «Информационная безопасность» в профессиональной деятельности; решать задачи профессиональной деятельности на основе норм права и с учетом основных требований информационной безопасности; **ОПК-3.2.3** ***Владеть:*** навыками использования информационно-коммуникационных технологий с учетом основных требований информационной безопасности; навыками выбора методов решения задач профессиональной деятельности на основе теоретических знаний в области информационной безопасности

ПК-2 Способен выполнять работы по созданию (модификации) и сопровождению информационных систем, автоматизирующих задачи организационного управления и бизнес-процессы	**ПК-2.1.** Выявляет требования к информационной системе и осуществляет адаптацию бизнес-процессов заказчика к возможностям типовой ИС	**ПК-2.1**.	**ПК-2.1.1** ***Знать:*** требования, предъявляемые к информационной системе осуществляющую адаптацию в реализации бизнес-процессов; **ПК-2.1.2** ***Уметь:*** адаптировать бизнес-процессы предприятия для обеспечения безопасности его ИТ-инфраструктуры; **ПК-2.1.3** ***Владеть:*** навыками выполнения работ, связанных с комплексным обеспечением информационной безопасности конкретных автоматизированных систем при адаптации бизнес-процессов;

2. Место учебной дисциплины в структуре образовательной программы

Блок:1. Дисциплины (модули) обязательной части ОП.

В структурной форме межпредметные связи изучаемой дисциплины указаны в соответствии с учебным планом образовательной программы по очной форме обучения.

Связь дисциплины «Информационная безопасность» с предшествующими дисциплинами и сроки их изучения

Код дисциплины	*Дисциплины, предшествующие дисциплине* «Информационная безопасность»	*Семестр*
Б1.В.01	Базы данных	4

Связь дисциплины «Информационная безопасность» со смежными дисциплинами, изучаемыми параллельно

Код дисциплины	*Дисциплины, изучаемые параллельно*	*Семестр*
Б1.О.30	Управление жизненным циклом информационных систем	5
Б1.В.04	Основы программирования в ИС	5
Б1.В.06	Автоматизация бизнес-процессов	5

Связь дисциплины «Информационная безопасность» с последующими дисциплинами и сроки их изучения

Код дисциплины	*Дисциплины, следующие за дисциплиной* «Информационная безопасность»	*Семестр*

Б1.О.33	Управление IT-проектами	7
Б1.В.06	Автоматизация бизнес-процессов	6
Б1.В.09	Конфигурирование и моделирование в системе "1С: Предприятие"	6
Б1.В.ДВ.02.01	Системы электронного документооборота	6
Б1.В.ДВ.02.02	Системы управления корпоративным контентом	6
Б1.В.ДВ.03.01	ИСУ предприятием ("1С: Предприятие")	8
Б1.В.ДВ.03.02	Программирование в 1С:	8
Б2.О.03(П)	Производственная практика: технологическая (проектно-технологическая) практика	6
Б2.О.04(Пд)	Производственная практика: преддипломная практика	8
Б2.В.01(П)	Производственная практика: практика по получению профессиональных умений и опыта профессиональной деятельности	7

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу

Виды учебной работы	**Форма обучения**	
	Очная	**Очно-заочная**
Порядковый номер семестра	5	5
Общая трудоемкость дисциплины всего (в з.е):	3	3
Контактная работа с преподавателем всего (в акад. часах), в том числе:	38	30
Занятия лекционного типа (лекции)	18	18
Лабораторные работы	-	-
Занятия семинарского типа (практические занятия, семинары в том числе в форме практической подготовки)	18	10
Текущая аттестация	1	1
Консультации (предэкзаменационные)	-	-
Промежуточная аттестация	1	1
Самостоятельная работа всего (в акад. часах), в том числе:	70	78
Форма промежуточной аттестации:		
зачет/ дифференцированный зачет	зачет	зачет
экзамен		
Общая трудоемкость дисциплины (в акад. часах)	108	108

4. Содержание дисциплины, структурированное по темам (разделам)

4.1. Тематическое планирование

Тема 1. Понятие информационной безопасности.

Основные составляющие информационной безопасности. Объектно-ориентированный подход к информационной безопасности. Требования, предъявляемые к информационной системе осуществляющую адаптацию в реализации бизнес-процессов

Тема 2. Законодательный уровень информационной безопасности.

Правовые акты общего назначения, затрагивающие вопросы информационной безопасности. Закон РФ "Об информации, информационных технологиях и о защите информации". Обзор зарубежного законодательства в области информационной безопасности.

Тема 3. Стандарты и спецификации в области информационной безопасности. Механизмы безопасности. Классы безопасности. Информационная безопасность распределенных систем.

Тема 4. Административный уровень информационной безопасности.
Политика безопасности. Администрирование средств безопасности. Синхронизация программы безопасности с жизненным циклом систем.

Тема 5. Управление рисками.
Подготовительные этапы управления рисками. Основные этапы управления рисками.

Тема 6. Процедурный уровень информационной безопасности.
Основные классы мер процедурного уровня. Физическая защита. Реагирование на нарушения режима безопасности.

Тема 7. Основные программно-технические меры информационной безопасности.
Особенности современных информационных систем с точки зрения безопасности. Архитектурная безопасность.

Тема 8. Моделирование, аудит, шифрование и контроль целостности.
Контроль целостности и цифровые сертификаты.

4.2. Содержание занятий семинарского типа

№	Содержание практических занятий	Виды практических занятий	Текущий контроль
1.	**Понятие информационной безопасности.** Организация защиты информации при передаче в телекоммуникационных сетях.	устный опрос по теме практического занятия;	Индивидуальное и групповое собеседование. Мониторинг практических заданий.
2.	**Законодательный уровень информационной безопасности.** Использование криптоалгоритмов в деятельности организации	устный опрос по теме практического занятия;	Индивидуальное и групповое собеседование. Мониторинг практических заданий.
3.	**Стандарты и спецификации в области информационной безопасности.** Создание и использование электронной подписи. Проверка принадлежности электронной цифровой подписи в электронном документе.	устный опрос по теме практического занятия;	Индивидуальное и групповое собеседование. Мониторинг практических заданий.
4.	**Административный уровень информационной безопасности.**	устный опрос по теме	Индивидуальное и групповое

	Состав и использование программных продуктов защиты информации.	практического занятия;	собеседование. Мониторинг практических заданий.
5.	**Управление рисками.** Анализ рисков информационной безопасности при организации защищенного документооборота в организации.	устный опрос по теме практического занятия;	Индивидуальное и групповое собеседование. Мониторинг практических заданий.
6.	**Процедурный уровень информационной безопасности.** Настройка и использование межсетевых экранов	устный опрос по теме практического занятия;	Индивидуальное и групповое собеседование. Мониторинг практических заданий.
7.	**Основные программно-технические меры информационной безопасности.** Использование современного стеганографического программного обеспечения для защиты авторских прав	устный опрос по теме практического занятия;	Индивидуальное и групповое собеседование. Мониторинг практических заданий.
8.	**Моделирование, аудит, шифрование и контроль целостности.** Анализ характеристик современных систем активного аудита	устный опрос по теме практического занятия	Индивидуальное и групповое собеседование. Мониторинг практических заданий.

4.3. Самостоятельная работа студента

№	Разделы и темы рабочей программы самостоятельного изучения	Перечень домашних заданий и других вопросов для самостоятельного изучения
1.	Основные составляющие информационной безопасности	- изучение литературы и других источников - подготовка сообщений к выступлению
2.	Криптографические способы защиты информации Написание, ввод, отладка и тестирование программ шифрования подстановкой и перестановкой	- изучение литературы и других источников - подготовка сообщений к выступлению
3.	Антивирусная защита Диагностика антивирусной программы и создание тестовых вирусов	- изучение литературы и других источников - подготовка сообщений к выступлению
4.	Сетевая безопасность Создание цифровой подписи	- изучение литературы и других источников - подготовка сообщений к выступлению

А) Творческое задание – частично регламентированное задание, имеющее нестандартное решение и позволяющее интегрировать знания различных областей, аргументировать собственную точку зрения. Может выполняться в индивидуальном порядке или группой обучающихся.
Частично регламентированное задание, имеющее нестандартное решение и позволяющее интегрировать знания различных областей, аргументировать собственную точку зрения. Может выполняться в индивидуальном порядке или группой обучающихся.

Примеры тем **творческих заданий** (доклад)

1. Основные принципами обеспечения информационной безопасности в ведущих зарубежных странах.
2. Построение концепции информационной безопасности предприятия.
3. Процедура аутентификации пользователя на основе пароля
4. Программная реализация криптографических алгоритмов.
5. Механизмы контроля целостности данных.

Б) Круглый стол - это форма организации обмена мнениями. Характер обмена мнениями при этом может быть различным.

Примерные темы для круглого стола

1. Применение на практике Доктрины информационной безопасности Российской Федерации.
2. Федеральные законы в области информации и информационной безопасности.
3. Указы президента РФ и постановления правительства РФ в области информации и информационной безопасности.
4. Правовые режимы защиты информации.
5. Правовые вопросы защиты информации с использованием технических средств.

В) Деловая игра - Совместная деятельность группы обучающихся под управлением преподавателя с целью решения учебных и профессионально-ориентированных задач путем игрового моделирования проблемной ситуации. Позволяет оценивать умение анализировать и решать типичные профессиональные задачи.

1 Тема (проблема) «Безопасность в сетях», «Угрозы современных интернет -ресурсов»
2. Концепция игры.
3 Роли: Каждая команда (в количестве 4-5 человек) получает проблемное задание, после выполнения которого публично защищает анкету хакера и пользователя сети.

Г) Контрольные работы - средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу учебной дисциплины.

Вариант 1

1. Понятие атрибутов доступа к файлам. Защита сетевого файлового ресурса на примерах организации доступа в различных операционных системах.

2. Понятие доступа к данным со стороны процесса; отличия от доступа со стороны пользователя. Понятие и примеры скрытого доступа. Надежность систем ограничения доступа.

Вариант 2

1. Современные программно-аппаратные средства защиты компьютерной информации.

2. Несанкционированное копирование программ как тип несанкционированного доступа. Юридические аспекты несанкционированного копирования программ. Способы защиты от копирования.

Вариант 3

1. Сравнительный анализ методов воздействия и противодействия в сети Internet.

2. Особенности построения защиты информации в телекоммуникационных сетях УИС.

Вариант 4

1. Методы и средства воздействия на безопасность телекоммуникационных сетей.

2. Направления по защите от враждебных воздействий на безопасность компьютерных сетей.

Вариант 5

1. Необходимые и достаточные условия предотвращения разрушающего воздействия вируса.

2. Угрозы безопасности современных информационно-вычислительных и телекоммуникационных сетей. Классификация угроз безопасности.

Вариант 6

1. Аппаратные и программно-аппаратные средства криптозащиты данных.

2. Вирусы как особый класс разрушающих программных воздействий. Защита от разрушающих программных воздействий.

Вариант 7

1. Понятие атрибутов доступа к файлам. Организация доступа к файлам в различных операционных системах

2. Способы фиксации фактов доступа. Журналы доступа. Выявление следов несанкционированного доступа к файлам

Вариант 8

1. Организационно-правовая основа защиты информации.

2. Методы и средства защиты данных от несанкционированного доступа.

Вариант 9

1. Необходимость, назначение и общее содержание организационно- правового обеспечения информационной безопасности.

2. Методы и специальные технические средства, используемые в ходе поисковой операции в целях обеспечения защиты информации.

Вариант 10

1. Понятие и цели проведения специальных проверок объектов информатизации; основные этапы проведения проверки

2. Уязвимость компьютерных систем. Понятие несанкционированного доступа (НСД). Классы и виды НСД .

Вариант 11

1. Требования и показатели защищенности автоматизированных средств обработки информации.

2. «Типовые» каналы утечки информации объектов информатизации УИС. Условия и факторы, способствующие утечке информации ограниченного доступа.

Вариант 12

1. Понятие и виды каналов утечки информации. «Типовые» каналы утечки информации объектов информатизации УИС.

2. Основные угрозы безопасности информации. Общая характеристика технических средств несанкционированного получения информации и технологий их применения.

4.4. Распределение часов по темам и видам учебных занятий

Номер раздела, темы дисциплины	***Компетенции***	***Контактная работа***		***Лекции***		***Практические занятия Семинары***		***Самост. работа студентов***	
Формы обучения		***ОФО***	***ОЗФО***	***ОФО***	***ОЗФО***	***ОФО***	***ОЗФО***	***ОФО***	***ОЗФО***
ТЕМА 1.	ОПК-3; ПК-2	6	8	4	6	2	2	8	8
ТЕМА 2.	ОПК-3; ПК-2	4		2		2		10	10
ТЕМА 3.	ОПК-3; ПК-2	4	6	2	4	2	2	8	10
ТЕМА 4.	ОПК-3; ПК-2	4		2		2		8	10
ТЕМА 5.	ОПК-3; ПК-2	6	4	2	2	4	2	10	10
ТЕМА 6.	ОПК-3; ПК-2	4	6	2	4	2	2	10	10
ТЕМА 7.	ОПК-3; ПК-2	4		2		2		8	10
ТЕМА 8.	ОПК-3; ПК-2	4	4	2	2	2	2	8	10
Текущая аттестация	ОПК-3; ПК-2	1							
Консультации (предэкзаменационные)		-							
Промежуточная аттестация	ОПК-3; ПК-2	1							
Всего:		***38***	***30***	***18***	***18***	***18***	***10***	***70***	***78***

4.5. Методические указания для обучающихся по освоению дисциплины

Для правильной организации самостоятельной работы необходимо учитывать порядок изучения разделов курса, находящихся в строгой логической последовательности. Поэтому хорошее усвоение одной части дисциплины является предпосылкой для успешного перехода к следующей. Для лучшего запоминания материала целесообразно использовать индивидуальные особенности и разные виды памяти: зрительную, слуховую, ассоциативную. Успешному запоминанию способствует приведение ярких свидетельств и наглядных примеров. Учебный материал должен постоянно повторяться и закрепляться.

Подготовка к практическому (семинарскому) занятию начинается с тщательного ознакомления с условиями предстоящей работы, т. е. с обращения к вопросам семинарских занятий. Определившись с проблемой, следует обратиться к рекомендуемой литературе. При подготовке к практическому (семинарскому) занятию обязательно требуется изучение дополнительной литературы по теме занятия. Без использования нескольких источников информации невозможно проведение дискуссии на занятиях, обоснование собственной позиции, построение аргументации. Если обсуждаемый аспект носит дискуссионный характер, следует изучить существующие точки зрения и выбрать тот подход, который вам кажется наиболее верным. При этом следует учитывать необходимость обязательной аргументации собственной позиции. Во время практических занятий рекомендуется активно участвовать в обсуждении рассматриваемой темы, выступать с подготовленными заранее докладами и презентациями, принимать участие в выполнении практических заданий.

С целью обеспечения успешного обучения студент должен готовиться к лекции, поскольку она является важной формой организации учебного процесса: знакомит с новым учебным материалом; разъясняет учебные элементы, трудные для понимания; систематизирует учебный материал; ориентирует в учебном процессе.

Подготовка к лекции заключается в следующем:

- внимательно прочитайте материал предыдущей лекции;
- узнайте тему предстоящей лекции (по тематическому плану);
- ознакомьтесь с учебным материалом по учебным пособиям;
- постарайтесь уяснить место изучаемой темы в своей профессиональной подготовке;
- запишите возможные вопросы, которые вы зададите преподавателю на лекции.

Во время лекции рекомендуется составлять конспект, фиксирующий основные положения лекции и ключевые определения по пройденной теме.

К зачету необходимо готовится целенаправленно, регулярно, систематически и с первых дней обучения по дисциплине. Попытки освоить дисциплину в период зачётно-экзаменационной сессией, как правило, показывают не слишком хороший результат. В самом начале учебного курса студенту следует познакомиться со следующей учебно-методической документацией:

- программой дисциплины;
- перечнем знаний и умений, которыми студент должен овладеть;
- тематическими планами лекций, семинарских занятий;
- контрольными мероприятиями;
- учебными пособиями по дисциплине;
- перечнем вопросов к зачету.

После этого у студента должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине. Систематическое выполнение учебной работы на лекциях, семинарских занятиях и в процессе самостоятельной работы позволит успешно освоить дисциплину и создать хорошую базу для сдачи зачета.

Рекомендуемая тематика занятий максимально полно реализуется в контактной работе со студентами очной формы обучения. В случае реализации образовательной программы в заочной / очно-заочной форме трудоемкость дисциплины сохраняется, однако объем учебного материала в значительной части осваивается студентами в форме самостоятельной работы. При этом требования к ожидаемым образовательным результатам студентов по данной дисциплине не зависят от формы реализации образовательной программы.

В случае организации учебной работы с использованием дистанционных образовательных технологий занятия проводятся в электронной информационно-образовательной среде института.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

5.1 Образовательные технологии

В освоении учебной дисциплины «Информационная безопасность» используются следующие **традиционные образовательные технологии:**

- чтение информационных лекций с использованием доски и видеоматериалов;
- практические/семинарские занятия;
- выполнение контрольных работ;
- выполнение творческих заданий;
- деловая игра;
- участие в работе круглого стола;
- контрольные опросы;
- консультации;
- самостоятельная работа студентов;
- тестирование;
- зачетная аттестация.

5.2.Использование информационных технологий:

- технологии, основанные на использовании ЭИОС института (методические материалы по дисциплине, размещенные на сайте ГСИ);
- Интернет-технологии;
- компьютерные обучающие и контролирующие программы;
- информационные технологии, позволяющие увеличить эффективность преподавания (за счет усиления иллюстративности):
  - ***лекция-визуализация –*** *иллюстративная форма проведения информационных и проблемных лекций;*
  - ***семинар-презентация*** *– использование студентами на семинарах специализированных программных средств.*

5.3. Активные и интерактивные методы и формы обучения

Из перечня видов: («мозговой штурм», анализ проблемных ситуаций, анализ конкретных

ситуаций, инциденты, имитация коллективной профессиональной деятельности, творческая работа, связанная с самопознанием и освоением дисциплины, деловая игра, круглый стол, диспут, дискуссия, мини-конференция и др.) используются следующие:
- «*мозговой штурм»;*
- *диспут* (способ ведения спора, проводимого с целью установления научной истины со ссылками на устоявшиеся письменные авторитетные источники и тщательный анализ аргументов каждой из сторон);
- *творческая работа;*
- *круглый стол;*
- *дискуссия (*как метод, активизирующий процесс обучения, изучения сложной темы, теоретической проблемы*) применяется на семинарах-дискуссиях, где обсуждаются спорные вопросы с выявлением мнений в студенческой группе;*
- *беседа.*

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Контроль качества освоения дисциплины включает в себя текущий контроль успеваемости и промежуточную аттестацию обучающихся. Промежуточная аттестация обучающихся по дисциплине проводится в форме зачета.

Конкретный перечень типовых контрольных заданий и иных материалов для оценки результатов освоения дисциплины, а также описание показателей и критериев оценивания компетенций приведен в фонде оценочных средств по дисциплине.

6.1. Формы текущего контроля

- *индивидуальное и групповое собеседование;*
- *мониторинг результатов практических занятий;*
- *выполнение творческих заданий;*
- *выполнение контрольных работ;*
- *выполнение практических работ;*
- *выполнение тестовых заданий;*

6.2. Тестовые задания:

См. приложение – «Банк тестов»

6.3. Форма промежуточного контроля по дисциплине –зачет

Вопросы к зачету:

1. Анализ угроз информационной безопасности.
2. Виды возможных нарушений информационной системы.
3. Общая классификация информационных угроз.
4. Виды угроз собственной информации в сфере финансовой деятельности.
5. Виды, принципы и действия вирусов, демаскирующие признаки.

6. Внутренние и внешние источники угроз информационной безопасности. Схема воздействия угроз на информационную систему.
7. Вредоносное программное обеспечение и методы борьбы с ним.
8. Инспектирование и анализ протоколов - как метод защиты информации.
9. Информационная безопасность при использовании средств связи.
10. Доктрина информационной безопасности Российской Федерации.
11. Классификация мероприятий по защите от несанкционированного доступа.
12. Классификация нарушителей по уровню возможностей.
13. Классификация современных стенографических методов защиты информации.
14. Контроль за действиями пользователя и событиями в сети.
15. Классические криптоалгоритмы - моноалфавитные подстановки.
16. Классические криптоалгоритмы - перестановки.
17. Межсетевые экраны – как метод защиты информации.
18. Меры противодействия угрозам собственной информации.
19. Место информационной безопасности в национальной безопасности Российской Федерации.
20. Методы обнаружения разрушающих программных средств.
21. Модели защиты информации в корпоративных системах.
22. Определение используемых руководящих документов и стандартов информационной безопасности.
23. Определение подходов к управлению рисками информационной безопасности.
24. Основные принципы защиты информационных технологий (четыре задачи системы защиты).
25. Виды паролей. Правила подбора паролей.
26. Парольные системы защиты.
27. Перечень основных формальных и неформальных средств защиты информации.
28. Политика безопасности и ее составляющие.
29. Фазы обращения информации в информационных системах.
30. Виды шифрования, применяемые в информационных системах.
31. Методы и типы аутентификации.
32. Правовое регулирование защиты информации.
33. Принципы восстановления информации и защиты после аварии.
34. Современные асимметричные системы шифрования. Обобщенная схема асимметричного шифрования.
35. Современные методы и средства обеспечения сетевой безопасности.

36. Современные программные угрозы, методы их обнаружения и предупреждения.

37. Современные симметричные системы шифрования. Обобщенная схема симметричного шифрования.

38. Способы контроля целостности данных.

39. Стандарты информационной безопасности.

40. Типовые удаленные атаки с использованием уязвимостей сетевых протоколов. Классификация удаленных атак.

41. Угрозы компьютерной информации, реализуемые на аппаратном уровне.

42. Управление рисками на различных стадиях жизненного цикла информационной системы. 43. Функциональное построение системы защиты информации организации и назначение основных подразделений.

44. Хранение информации. Сжатие и защита информации при хранении.

45. Цели и задачи обеспечения информационной безопасности.

46. Цифровая подпись.

47. Цифровые водяные знаки.

48. Электронная цифровая подпись. Обобщенная схема постановки и её проверки.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

7.1. Рекомендуемая литература

Основная литература

Балдин, К. В. Информационные системы в экономике : учебник / К. В. Балдин, В. Б. Уткин. — 9-е изд., стер. — Москва : Дашков и К°, 2021. — 395 с. : ил., табл. — ISBN 978-5-394-04038-2. — Текст : электронный // Университетская библиотека ONLINE : [сайт]. — URL: https://biblioclub.ru/index.php?page=book&id=684194

Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт : [сайт]. — URL: https://urait.ru/bcode/531084

Дополнительная литература

Жарова, А. К. Правовое регулирование создания и использования информационной инфраструктуры в Российской Федерации : монография / А. К. Жарова. — Москва : Издательство Юрайт, 2023. — 301 с. — (Актуальные монографии). — ISBN 978-5-534-14919-7. — Текст : электронный // Образовательная платформа Юрайт : [сайт]. — URL: https://urait.ru/bcode/519998

Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт : [сайт]. — URL: https://urait.ru/bcode/513300

Технологии обеспечения безопасности информационных систем : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. — Москва : Директ-Медиа, 2021. — 210 с. : ил., схем., табл. — ISBN 978-5-4499-1671-6. — Текст : электронный // Университетская библиотека ONLINE : [сайт]. — URL: https://biblioclub.ru/index.php?page=book&id=598988

Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // Образовательная платформа Юрайт : [сайт]. — URL: https://urait.ru/bcode/518441

Периодическая литература (библиотека ГСИ)

1. Информатизация и связь.
2. Проблемы управления.
3. Российский журнал менеджмента.
4. Системный администратор.

ЭБС IPR BOOKS:

1. Актуальные проблемы экономики и менеджмента (доступный архив: 2019–2021). – URL: https://www.iprbookshop.ru/98831.html.

2. Вестник Российского университета дружбы народов. Серия Экономика (доступный архив: 2011–2022). – URL: https://www.iprbookshop.ru/32735.html.

3. Вестник Ростовского государственного экономического университета (РИНХ) (доступный архив: 2014–2022). – URL: https://www.iprbookshop.ru/61941.html.

4. Вестник Сибирского института бизнеса и информационных технологий (доступный архив: 2019–2022). – URL: https://www.iprbookshop.ru/102212.html.

5. Известия Саратовского университета. Новая серия. Серия Математика. Механика. Информатика (доступный архив: 2019–2022). – URL: https://www.iprbookshop.ru/99689.html.

6. Прикладная информатика (доступный архив: 2006–2022). – URL: https://www.iprbookshop.ru/11770.html.

7. Программные продукты и системы (доступный архив: 2010–2022). – URL: https://www.iprbookshop.ru/25852.html.

8. Современная конкуренция (доступный архив: 2007–2022). – URL: https://www.iprbookshop.ru/11778.html.

9. Стратегии бизнеса (доступный архив: 2020–2022). – URL: https://www.iprbookshop.ru/106278.html.

7.2. Электронные образовательные и информационные ресурсы

1. Электронно-библиотечная система «ЮРАЙТ» - https://urait.ru/
2. Университетская библиотека онлайн – www/biblioclub.ru

7.3. Профессиональные базы данных и информационные справочные системы

Информационно-справочные системы

1. «Система КонсультантПлюс» – компьютерная справочная правовая система - http://www.consultant.ru/
2. «Гарант» – справочно-правовая система по законодательству Российской Федерации - http://www.garant.ru/

3. Единое окно доступа к образовательным ресурсам. - http://window.edu.ru/
4. Национальная информационно-аналитическая система Российский индекс научного цитирования (РИНЦ). - https://www.elibrary.ru
5. Федеральный портал «Российское образование» - http://www.edu.ru/

Профессиональные базы данных

1. Научная электронная библиотека eLibrary.ru - Российский индекс научного цитирования (РИНЦ)
2. Открытый портал информационных ресурсов (научных статей, сборников работ и монографий по различным направлениям наук) https://elibrary.ru/project_risc.asp
3. База данных научных журналов на русском и английском языке ScienceDirect
4. Открытый доступ к метаданным научных статей по различным направлениям наук поиск рецензируемых журналов, статей, глав книг и контента открытого доступа http://www.sciencedirect.com/
5. Федеральный портал «Российское образование» http://www.edu.ru/
6. Бесплатная электронная библиотека онлайн «Единое окно доступа к образовательным ресурсам» http://window.edu.ru/
7. Единая коллекция цифровых образовательных ресурсов Научно-практические и методические материалы http://school-collection.edu.ru/
8. Единый реестр российских программ для электронных вычислительных машин и баз данных, в том числе свободно распространяемых, доступен по ссылке Reestr-Minsvyaz.ru
9. Сайт, посвященный SQL, программированию, базам данных, разработке информационных систем https://www.sql.ru/
10. На сайте проекта OpenNet размещается информация о Unix системах и открытых технологиях для администраторов, программистов и пользователей http://www.opennet.ru/
11. Библиотека программиста https://proglib.io
12. Сообщество IT-Специалистов https://habr.com/ru/
13. Сеть разработчиков Microsoft https://msdn.microsoft.com/ru-ru/
14. Сборник статей по информационной безопасности http://www.iso27000.ru/chitalnyi-zai

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Министерство образования и науки Российской Федерации. 100% доступ - http://минобрнауки.рф/
2. Федеральная служба по надзору в сфере образования и науки. 100% доступ - http://obrnadzor.gov.ru/
3. Федеральный портал «Российское образование». 100% доступ - http://www.edu.ru/
5. Федеральный центр информационно-образовательных ресурсов. 100% доступ - http://fcior.edu.ru/
6. Электронно-библиотечная система, содержащая полнотекстовые учебники, учебные пособия, монографии и журналы в электронном виде 5100 изданий открытого доступа. 100% доступ - http://bibliorossica.com/
7. Федеральная служба государственной статистики. 100% доступ - http://www.gks.ru

8. Программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Microsoft Windows 10,
Microsoft Office (Word, Excel, PowerPoint, Outlook, Publisher),

Антивирус Windows Defender (входит в состав операционной системы Microsoft Windows)

Программное обеспечение отечественного производства

INDIGO
Яндекс.Браузер

Свободно распространяемое программное обеспечение

Adobe Reader для Windows
Архиватор HaoZip

9. Материально-техническое обеспечение, необходимое для осуществления образовательного процесса по дисциплине

Для проведения учебных занятий используются учебные аудитории, оснащенные оборудованием и техническими средствами обучения: специализированной мебелью, отвечающей всем установленным нормам и требованиям; ПК, переносная аудио и видеоаппаратура (проектор, экран, персональный компьютер или ноутбук с необходимым программным обеспечением для тематических иллюстраций и демонстраций, соответствующих программе дисциплины), телевизором.

Для самостоятельной работы обучающихся используются помещения, оснащенные компьютерной техникой: персональные компьютеры с доступом к сети Интернет и ЭИОС института, принтеры; специализированной мебелью, отвечающей всем установленным нормам и требованиям.

Для обучения инвалидов и лиц с ограниченными возможностями здоровья институтом могут быть представлены специализированные средства обучения, в том числе технические средства коллективного и индивидуального пользования.

10. Методические рекомендации по обучению лиц с ограниченными возможностями здоровья

Профессорско-педагогический состав знакомится с психолого-физиологическими особенностями обучающихся инвалидов и лиц с ограниченными возможностями здоровья, индивидуальными программами реабилитации инвалидов (при наличии). При необходимости осуществляется дополнительная поддержка преподавания тьюторами, психологами, социальными работниками, прошедшими подготовку ассистентами.

В соответствии с методическими рекомендациями Минобрнауки РФ (утв. 8 апреля 2014 г. N АК-44/05вн) в курсе предполагается использовать социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Подбор и разработка учебных материалов производятся с учетом предоставления материала в различных формах: аудиальной, визуальной, с использованием специальных технических средств и информационных систем.

Освоение дисциплины лицами с ОВЗ осуществляется с использованием средств обучения общего и специального назначения (персонального и коллективного использования). Материально-техническое обеспечение предусматривает приспособление аудиторий к нуждам лиц с ОВЗ.

Форма проведения аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей. Для студентов с ОВЗ предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной или электронной форме (для лиц с нарушениями опорно-двигательного аппарата);
- в печатной форме или электронной форме с увеличенным шрифтом и контрастностью (для лиц с нарушениями слуха, речи, зрения);
- методом чтения ассистентом задания вслух (для лиц с нарушениями зрения).

Студентам с инвалидностью увеличивается время на подготовку ответов на контрольные вопросы. Для таких студентов предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге или набором ответов на компьютере (для лиц с нарушениями слуха, речи);
- выбором ответа из возможных вариантов с использованием услуг ассистента (для лиц с нарушениями опорно-двигательного аппарата);
- устно (для лиц с нарушениями зрения, опорно-двигательного аппарата).

При необходимости для обучающихся с инвалидностью процедура оценивания результатов обучения может проводиться в несколько этапов.

ПРИЛОЖЕНИЕ 1

Тесты.
Способствует закреплению прочных знаний и формированию понятийного аппарата студентов по дисциплине. Состоит во внимательном и всестороннем обдумывании сущности и содержания всех ответов на каждый из поставленных вопросов и выбор одного (или нескольких) правильных. Критерии оценки зависят от количества выбранных правильных ответов. Рекомендуется:

1. Выполнять задания в предложенной последовательности, внимательно прочитав указания.
2. Не задерживаться слишком долго на одном задании. Если возникают затруднения, переходите к следующему.
3. Прежде чем сдать работу преподавателю, проверьте ответы.

«БАНК ТЕСТОВ»

Защита информации это:
1. процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
2. преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
3. получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
4. совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
5. деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:
1. активный перехват;
2. пассивный перехват;
3. аудио-перехват;
4. видео-перехват;
5. просмотр мусора.

Что такое несанкционированный доступ (нсд)?
1. Доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа
2.Создание резервных копий в организации
3. Правила и положения, выработанные в организации для обхода парольной защиты
4. Вход в систему без согласования с руководителем организации

К посторонним лицам нарушителям информационной безопасности относится:
а) персонал, обслуживающий технические средства;
б) технический персонал, обслуживающий здание; в) сотрудники службы безопасности.
г) представители конкурирующих организаций.

К внутренним нарушителям информационной безопасности относится:
а) любые лица, находящиеся внутри контролируемой территории;

б) персонал, обслуживающий технические средства.
в) сотрудники отделов разработки и сопровождения ПО;
г) технический персонал, обслуживающий здание

Собственником информации не может быть:
а) государство;
б) юридическое лицо;
в) группа физических лиц;
г) физическое лицо;
д) ответы, а – г правильны;
е) нет правильного ответа.

Заранее намеченный результат защиты информации – это
а) замысел защиты информации;
б) цель защиты информации;
в) уровень эффективности защиты информации.

Кто является основным ответственным за определение уровня классификации информации?
а) Руководитель среднего звена
б) Высшее руководство
в) Владелец
г) Пользователь

Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
а) Сотрудники
б) Хакеры
в) Атакующие
г) Контрагенты (лица, работающие по договору)

Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
в) Улучшить контроль за безопасностью этой информации
г) Снизить уровень классификации этой информации

Что самое главное должно продумать руководство при классификации данных?
а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
б) Необходимый уровень доступности, целостности и конфиденциальности
в) Оценить уровень риска и отменить контрмеры
г) Управление доступом, которое должно защищать данные

Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
а) Владельцы данных
б) Пользователи

в) Администраторы
г) Руководство

Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
а) Поддержка высшего руководства
б) Эффективные защитные меры и методы их внедрения в) Актуальные и адекватные политики и процедуры безопасности
г) Проведение тренингов по безопасности для всех сотрудников

Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
а) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
б) Когда риски не могут быть приняты во внимание по политическим соображениям
в) Когда необходимые защитные меры слишком сложны
г) Когда стоимость контрмер превышает ценность актива и потенциальные потери

Что такое политики безопасности?
а) Пошаговые инструкции по выполнению задач безопасности
б) Общие руководящие требования по достижению определенного уровня безопасности
в) Широкие, высокоуровневые заявления руководства
г) Детализированные документы по обработке инцидентов безопасности