Министерство науки и высшего образования Российской Федерации
Филиал Федерального государственного бюджетного образовательного учреждения высшего образования
«Кубанский государственный университет»
в г.Тихорецке

Кафедра социально-гуманитарных дисциплин

УТВЕРЖДАЮ:
Проректор по работе с филиалами
_____ А.А. Евдокимов
_____ 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.08 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ (ОРГАНИЗАЦИИ)

Направление подготовки 38.03.01 Экономика
Направленность (профиль) Экономика предприятий и организаций
Форма обучения: очная, очно-заочная
Квалификация: бакалавр
Год начала подготовки: 2023

Тихорецк 2023

Рабочая программа дисциплины составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 38.03.01 Экономика

Программу составил:
Доцент кафедры социально-гуманитарных дисциплин, канд. пед. наук, доц. Е.А. Дегтярева

Рабочая программа дисциплины утверждена на заседании кафедры социально-гуманитарных дисциплин (разработчика)
Протокол № 9 от 24 мая 2023 г.
Заведующий кафедрой, канд. экон. наук, доц. Е.В. Мезенцева

Рабочая программа дисциплины обсуждена на заседании кафедры экономики и менеджмента (выпускающей)
Протокол № 9 от 24 мая 2023 г.
Заведующий кафедрой, д-р экон. наук, доц. Е.В. Королюк

Утверждена на заседании учебно-методической комиссии филиала по УГН «Экономика и управление»
Протокол № 2 от 24 мая 2023 г.
Председатель УМК, канд. экон. наук, доц. М.Г. Иманова

Рецензенты:

Э.П. Черняева, зав. кафедрой математики и информатики филиала ФГБОУ ВО КубГУ в г. Армавире, канд. пед. наук

В.Е. Беличенко, заведующий кафедрой информатики и информационных технологий обучения ФГБОУ ВО «Армавирский государственный педагогический университет», канд. тех. наук, доц.

1 ЦЕЛИ И ЗАДАЧИ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

1.1 Цель освоения дисциплины: формирование знаний о сущности информационной безопасности, ее роли в системе управления предприятием в условиях рыночных отношений, сущности и характере угроз в информационной сфере, а также формирование умений и навыков по реализации, способов и средств защиты информации на предприятии.

1.2 Задачи дисциплины:

– изучение основных понятий в области защиты информации, принципов обеспечения безопасности информации на предприятии;

– изучение основных видов информации ограниченного доступа, правил формирования соответствующего перечня информационных ресурсов;

– изучение актуальных угроз безопасности информации, характерных для обработки в информационных системах современных предприятий и организаций различных форм собственности;

– изучение современных способов и средств защиты информации, в том числе информации, составляющей государственную тайну, требований по применению данных способов и средств в целях обеспечения безопасности информации на предприятии;

– формирование умений по разработке перечня информации ограниченного доступа в соответствии с особенностями деятельности предприятия;

– формирование умений анализа актуальных угроз безопасности, их классификации и оценки с точки зрения возможного ущерба для деятельности предприятия;

– формирование навыков осуществления выбора правовых, организационных и технических средств защиты информации для выполнения требований по обеспечению безопасности информации, в том числе информации, составляющей государственную тайну.

1.3 Место дисциплины (модуля) в структуре образовательной программы

Данная дисциплина относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины (модули)» учебного плана.

В соответствии с рабочим учебным планом дисциплина изучается на 3 курсе по очной и очно-заочной форме обучения. Вид промежуточной аттестации: зачет.

Предшествующими дисциплинами, необходимыми для изучения курса, являются дисциплины «Компьютерный практикум», «Информационно-коммуникационные технологии в профессиональной деятельности», «Профессиональные компьютерные программы», а последующей дисциплиной для которой данная дисциплина является предшествующей в соответствии с учебным планом - «Информационные технологии в управлении предприятием (организации)».

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование индикатора	Результаты обучения по дисциплине
ПК-2. Способен формировать и прогнозировать цены на товары, работы и услуги	
ИПК-2.5. Соблюдает конфиденциальность информации	Знает принципы обеспечения безопасности информации на предприятии и правила формирования перечня сведений конфиденциального характера. Знает актуальные угрозы безопасности информации и современные способы и средства защиты информации на предприятии. Знает о необходимости неразглашения материалов рабочих исследований и о нераспространении сведений, порочащих иные организации и коллег, не допущения клеветы и распространения сведений, порочащих иные организации и коллег, соблюдения конфиденциальности информации и не разглашения

Код и наименование индикатора	Результаты обучения по дисциплине
	материалов рабочих исследований
	Умеет анализировать и классифицировать актуальные угрозы безопасности информации и оценивать их с точки зрения возможного ущерба для деятельности предприятия. Умеет осуществлять выбор правовых, организационных и технических средств защиты информации для выполнения требований по обеспечению безопасности информации
	Владеет навыками сбора и обработки информации с учетом требований информационной безопасности. Владеет навыками применения информационно-коммуникационных технологий к решению задач профессиональной деятельности с учетом требований информационной безопасности

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2 СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 2 зач.ед. (108 час.), их распределение по видам работ представлено в таблице.

Вид работ		Форма обучения			
		очная		очно-заочная	
		всего часов	5 семестр	всего часов	5 семестр
Контактная работа, в том числе:		**38,2**	**38,2**	**28,2**	**28,2**
Аудиторные занятия (всего):		**34**	**34**	**24**	**24**
Занятия лекционного типа		18	18	12	12
Лабораторные занятия		16	16	12	12
Семинарские занятия					
Иная контактная работа:		**4,2**	**4,2**	**4,2**	**4,2**
Контроль самостоятельной работы (КСР)		4	4	4	4
Промежуточная аттестация (ИКР)		0,2	0,2	0,2	0,2
Самостоятельная работа, в том числе:		**33,8**	**33,8**	**43,8**	**43,8**
Курсовая работа					
Контрольная работа					
Расчетно-графическая работа					
Реферат/эссе (подготовка)		3,8	3,8	3,8	3,8
Самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам и т.д.)		30	30	40	40
Подготовка к текущему контролю					
Контроль:					
Подготовка к экзамену					
Общая трудоемкость	**час.**	**72**	**72**	**72**	**72**
	в том числе	**38,2**	**38,2**	**28,2**	**28,2**

	контактная работа				
	зач. ед	**2**	**2**	**2**	**2**

2.2 Содержание дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 5 семестре (очная форма обучения)

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	Информационная безопасность. Комплексный подход. Место информационной безопасности в системе национальной безопасности России.	15,8	4		2	9,8
2	Основы информационной безопасности организации.	8	2		2	4
3	Защита информации.	6	2		2	2
4	Основные свойства и состав защищаемой информации.	6	2		2	2
5	Институты информации ограниченного доступа.	8	2		2	4
6	Источники и способы реализации угроз безопасности информации. Уязвимости систем обработки информации.	8	2		2	4
7	Каналы утечки информации и методы несанкционированного доступа к информации ограниченного доступа.	8	2		2	4
8	Комплексная система защиты информации на предприятии.	8	2		2	4
	ИТОГО по разделам дисциплины	*67,8*	*18*		*16*	*33,8*
	Контроль самостоятельной работы (КСР)	4				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю					
	Общая трудоемкость по дисциплине	72				

Разделы дисциплины, изучаемые в 5 семестре (очно-заочная форма)

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1	Информационная безопасность. Комплексный подход. Место информационной безопасности в системе национальной безопасности России.	11,8	2		2	7,8
2	Основы информационной безопасности организации.	9	1		2	6
3	Защита информации.	5	1			4
4	Основные свойства и состав защищаемой информации.	8	2		2	4
5	Институты информации ограниченного доступа.	8	2		2	4

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
6	Источники и способы реализации угроз безопасности информации. Уязвимости систем обработки информации.	7	1		2	4
7	Каналы утечки информации и методы несанкционированного доступа к информации ограниченного доступа.	9	1			8
8	Комплексная система защиты информации на предприятии.	10	2		2	6
	ИТОГО по разделам дисциплины	*67,8*	*12*		*12*	*43,8*
	Контроль самостоятельной работы (КСР)	4				
	Промежуточная аттестация (ИКР)	0,2				
	Подготовка к текущему контролю					
	Общая трудоемкость по дисциплине	72				

2.3 Содержание разделов (тем) дисциплины

В данном подразделе приводится описание содержания дисциплины, структурированное по разделам, с указанием по каждому разделу формы текущего контроля: В – вопросы для устного опроса; Л- лабораторная работа; Р – реферат, Т – тесты.

2.3.1 Занятия лекционного типа

Очная форма обучения

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	Тема 1. Информационная безопасность. Комплексный подход. Место информационной безопасности в системе национальной безопасности России.	Проблема информационной безопасности на современном этапе. Понятие информационной безопасности. Основные составляющие информационной безопасности. Система информационной безопасности. Её объекты.	В
2	Тема 1. Информационная безопасность. Комплексный подход. Место информационной безопасности в системе национальной безопасности России.	Информационная война как угроза национальной безопасности. Понятие национальной безопасности РФ. Место информационной безопасности в системе национальной безопасности. Значение информационной безопасности для субъектов информационных отношений. Роль информационной безопасности в обеспечении национальной безопасности государства	В
3	Тема 2. Основы информационной безопасности организации	Концептуальная модель информационной безопасности организации и основные понятия. Объекты и угрозы информационной безопасности организации. Политика обеспечения информационной безопасности организации. Система обеспечения информационной безопасности организации.	В
4	Тема 3. Защита информации	Система понятий в области защиты информации. Направления и относящиеся к ним способы защиты информации. Концептуальная модель защиты информации.	В

№	Наименование раздела	Содержание раздела	Форма текущего контроля
5	Тема 4. Основные свойства и состав защищаемой информации	Основные свойства информации с точки зрения обеспечения ее безопасности. Понятие и состав защищаемой информации. Принципы отнесения информации к защищаемой. Носители защищаемой информации.	В
6	Тема 5. Институты информации ограниченного доступа	Классификация информации ограниченного доступа по видам тайны. Государственная тайна. Коммерческая тайна. Персональные данные. Служебная тайна. Профессиональная тайна.	В
7	Тема 6. Источники и способы реализации угроз безопасности информации. Уязвимости систем обработки информации	Понятие угрозы безопасности информации. Общая классификация угроз. Источники угроз безопасности информации. Виды угроз безопасности информации. Уязвимости систем обработки информации. Классификация уязвимостей.	В
8	Тема 7. Каналы утечки информации и методы несанкционированного доступа к информации ограниченного доступа	Каналы утечки информации ограниченного доступа. Методы несанкционированного доступа к конфиденциальной информации с использованием различных каналов. Неформальная модель нарушителя безопасности автоматизированных систем.	В
9	Тема 8. Комплексная система защиты информации на предприятии	Понятие и общая структура комплексной системы защиты информации на предприятии. Компоненты комплексной системы защиты информации на предприятии, их назначение и стандартизация. Требования к системам защиты информации автоматизированных систем.	В

Очно-заочная форма обучения

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	Тема 1. Информационная безопасность. Комплексный подход. Место информационной безопасности в системе национальной безопасности России.	Проблема информационной безопасности на современном этапе. Понятие информационной безопасности. Основные составляющие информационной безопасности. Система информационной безопасности. Её объекты. Место информационной безопасности в системе национальной безопасности. Значение информационной безопасности для субъектов информационных отношений. Роль информационной безопасности в обеспечении национальной безопасности государства	В
2	Тема 2. Основы информационной безопасности организации	Концептуальная модель информационной безопасности организации и основные понятия. Объекты и угрозы информационной безопасности организации. Политика обеспечения информационной безопасности организации. Система обеспечения информационной безопасности организации.	В
	Тема 3. Защита информации	Система понятий в области защиты информации. Направления и относящиеся к ним способы защиты информации. Концептуальная модель защиты информации.	В
3	Тема 4. Основные свойства	Основные свойства информации с точки зрения	В

№	Наименование раздела	Содержание раздела	Форма текущего контроля
	и состав защищаемой информации	обеспечения ее безопасности. Понятие и состав защищаемой информации. Принципы отнесения информации к защищаемой. Носители защищаемой информации.	
4	Тема 5. Институты информации ограниченного доступа	Классификация информации ограниченного доступа по видам тайны. Государственная тайна. Коммерческая тайна. Персональные данные. Служебная тайна. Профессиональная тайна.	В
5	Тема 6. Источники и способы реализации угроз безопасности информации. Уязвимости систем обработки информации	Понятие угрозы безопасности информации. Общая классификация угроз. Источники угроз безопасности информации. Виды угроз безопасности информации. Уязвимости систем обработки информации. Классификация уязвимостей.	В
	Тема 7. Каналы утечки информации и методы несанкционированного доступа к информации ограниченного доступа	Каналы утечки информации ограниченного доступа. Методы несанкционированного доступа к конфиденциальной информации с использованием различных каналов. Неформальная модель нарушителя безопасности автоматизированных систем.	В
6	Тема 8. Комплексная система защиты информации на предприятии	Понятие и общая структура комплексной системы защиты информации на предприятии. Компоненты комплексной системы защиты информации на предприятии, их назначение и стандартизация. Требования к системам защиты информации автоматизированных систем.	В

2.3.2 Занятия семинарского типа (практические / семинарские занятия/ лабораторные работы)

Очная форма обучения

№	Наименование раздела	Тематика лабораторных занятий	Форма текущего контроля
1	Тема 1. Информационная безопасность. Комплексный подход. Место информационной безопасности в системе национальной безопасности России.	Лабораторная работа №1. Изучение основных положений Федерального закона "Об информации, информационных технологиях и о защите информации", «О государственной тайне».	Л,Т
2	Тема 2. Основы информационной безопасности организации.	Лабораторная работа №2. Изучение способов защиты текстовых документов в Microsoft Word. Изучение способов защиты баз данных в Microsoft Access.	Л,Т
3	Тема 3. Защита информации.	Лабораторная работа №3. Изучение методов парольной защиты документов табличного процессора MS Excel. Архивирование данных как средство защиты данных.	Л,Т
4	Тема 4. Основные свойства и состав защищаемой информации.	Лабораторная работа №4. Изучение основных положений Федерального закона «О коммерческой тайне», «О персональных данных». Закрепление права предприятия на защиту информации в нормативных документах.	Л,Т
5	Тема 5. Институты	Лабораторная работа №5. Знакомство с	Л,Т

№	Наименование раздела	Тематика лабораторных занятий	Форма текущего контроля
	информации ограниченного доступа.	криптографическими методами защиты информации. Шифрование методом перестановки и замены.	
6	Тема 6. Источники и способы реализации угроз безопасности информации. Уязвимости систем обработки информации.	Лабораторная работа №6. Знакомство с системой защиты Windows, с системой безопасности удаленного доступа, со средствами защиты информации в операционной системе Windows.	Л,Т
7	Тема 7. Каналы утечки информации и методы несанкционированного доступа к информации ограниченного доступа.	Лабораторная работа №7. Знакомство с криптографическими методами защиты информации. Шифрование методом алгебры матриц.	Л,Т
8	Тема 8. Комплексная система защиты информации на предприятии.	Лабораторная работа №8. Применение программных средств антивирусной защиты в компьютерных системах. Антивирусные программы и утилиты	Л,Р, Т

Очно-заочная форма обучения

№	Наименование раздела	Тематика лабораторных занятий	Форма текущего контроля
1	Тема 1. Информационная безопасность. Комплексный подход. Место информационной безопасности в системе национальной безопасности России.	Лабораторная работа №1. Изучение основных положений Федерального закона "Об информации, информационных технологиях и о защите информации", «О государственной тайне».	Л,Т
2	Тема 2. Основы информационной безопасности организации.	Лабораторная работа №2. Изучение способов защиты текстовых документов в Microsoft Word. Изучение способов защиты баз данных в Microsoft Access. Изучение методов парольной защиты документов табличного процессора MS Excel.	Л,Т
3	Тема 4. Основные свойства и состав защищаемой информации.	Лабораторная работа №4. Изучение основных положений Федерального закона «О коммерческой тайне», «О персональных данных». Закрепление права предприятия на защиту информации в нормативных документах.	Л,Т
4	Тема 5. Институты информации ограниченного доступа.	Лабораторная работа №5. Знакомство с криптографическими методами защиты информации. Шифрование методом перестановки и замены.	Л,Т
5	Тема 6. Источники и способы реализации угроз безопасности информации. Уязвимости систем обработки информации.	Лабораторная работа №6. Знакомство с системой защиты Windows, с системой безопасности удаленного доступа, со средствами защиты информации в операционной системе Windows.	Л,Т
6	Тема 8. Комплексная система защиты информации на предприятии.	Лабораторная работа №7. Применение программных средств антивирусной защиты в компьютерных системах. Антивирусные программы и утилиты	Л,Р, Т

При изучении дисциплины могут применяться электронное обучение, дистанционные образовательные технологии в соответствии с ФГОС ВО.

2.3.4 Примерная тематика курсовых работ (проектов)

Курсовые работы не предусмотрены

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	Проработка учебного (теоретического) материала	Самостоятельная работа студентов: методические рекомендации для бакалавров направления подготовки 38.03.01 Экономика, утвержденные кафедрой экономики и менеджмента (протокол №9 от 24.05.2023 г.)
2	Подготовка к текущему контролю	
3	Подготовка рефератов	Письменные работы студентов: методические рекомендации для бакалавров направления подготовки 38.03.01 Экономика, утвержденные кафедрой экономики и менеджмента (протокол №9 от 24.05.2023 г.)
4	Выполнение упражнений	
5	Выполнение лабораторной работы	Лабораторные работы студентов: методические рекомендации для бакалавров направления подготовки 38.03.01 Экономика, утвержденные кафедрой экономики и менеджмента (протокол №9 от 24.05.2023 г.)

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа,

– в форме аудиофайла,

– в печатной форме на языке Брайля.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа,

– в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3 ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ, ПРИМЕНЯЕМЫЕ ПРИ ОСВОЕНИИ ДИСЦИПЛИНЫ

В ходе изучения дисциплины предусмотрено использование следующих образовательных технологий: лекции, практические занятия, проблемное обучение, самостоятельная работа студентов.

Компетентностный подход в рамках преподавания дисциплины реализуется в использовании интерактивных технологий и активных методов (разбора конкретных ситуаций, моделирование предметного и социального содержания будущей профессиональной деятельности) в сочетании с внеаудиторной работой.

Информационные технологии, применяемые при изучении дисциплины: использование информационных ресурсов, доступных в информационно-телекоммуникационной сети Интернет.

Адаптивные образовательные технологии, применяемые при изучении дисциплины – для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Информационная безопасность предприятия (организации)».

Оценочные средства включает контрольные материалы для проведения **текущего контроля** в форме вопросов для устного опроса; упражнений и задач; рефератов, тестовых заданий и **промежуточной аттестации** в форме вопросов к зачету.

№ п/п	Код и наименование индикатора (в соответствии с п. 1.4)	Результаты обучения (в соответствии с п. 1.4)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	**ИОПК-2.5** Соблюдает конфиденциальность информации	Знает принципы обеспечения безопасности информации на предприятии и правила формирования перечня сведений конфиденциального характера. Знает актуальные угрозы безопасности информации и современные способы и средства защиты информации на предприятии. Знает о необходимости неразглашения материалов рабочих исследований и о нераспространении сведений, порочащих иные организации и коллег, не допущения клеветы и распространения сведений, порочащих иные организации и коллег, соблюдения конфиденциальности информации и не разглашения материалов рабочих исследований. Умеет анализировать и классифицировать актуальные угрозы безопасности информации и оценивать их с точки зрения возможного ущерба для деятельности предприятия. Умеет осуществлять выбор правовых, организационных и технических средств защиты информации для выполнения требований по обеспечению безопасности информации. Владеет навыками сбора и обработки информации с учетом требований информационной безопасности. Владеет навыками применения информационно-коммуникационных технологий к решению задач профессиональной	Вопросы для устного опроса, лабораторные работы, рефераты, тесты	Вопросы к зачету 1-31

№ п/п	Код и наименование индикатора (в соответствии с п. 1.4)	Результаты обучения (в соответствии с п. 1.4)	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
		деятельности с учетом требований информационной безопасности		

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерные вопросы для устного опроса

Тема 6. Источники и способы реализации угроз

1. Дать определение понятию угрозы утраты информации.
2. Кратко классифицируйте угрозы безопасности информации.
3. Перечислить каналы несанкционированного доступа к информации (НСДИ).
4. Перечислить методы несанкционированного доступа к информации.
5. Перечислите виды объективных источников угрозы информации.
6. Перечислите виды субъективных источников угрозы информации.
7. Перечислите классы уязвимостей систем обработки информации. Дайте их краткую характеристику.
8. Перечислить элементы системы защиты информации.

Примерные темы рефератов

Тема 8. Комплексная система защиты информации на предприятии

1. Информационное право и концепция информационной безопасности.
2. Основы экономической безопасности предпринимательской деятельности.
3. Экономические основы защиты конфиденциальной информации.
4. Организационные основы защиты конфиденциальной информации.
5. Составление инструкции по обработке и хранению конфиденциальных документов.
6. Архивное хранение конфиденциальных документов.
7. Порядок подбора персонала для работы с конфиденциальной информацией.
8. Методика тестирования и проведения собеседования с претендентами на должность, связанную с секретами фирмы.
9. Порядок проведения переговоров и совещаний по конфиденциальным вопросам.
10. Организационное обеспечение защиты информации, обрабатываемой средствами вычислительной и организационной техники.
11. Направления и методы защиты профессиональной тайны.
12. Направления и методы защиты служебной тайны.
13. Направления и методы защиты персональных данных о гражданах.

Примерные задания к лабораторным работам

Тема 5. Институты информации ограниченного доступа.

Лабораторная работа №5. Знакомство с криптографическими методами защиты информации.

Цель работы: изучение методов шифрования методом перестановки и замены.

Для обеспечения защиты информации в настоящее время не существует какого-то одного технического приема или средства, однако общим в решении многих проблем безопасности является использование криптографии и криптоподобных преобразований информации.

Процессы шифрования и расшифрования осуществляются в рамках некоторой криптосистемы. Для **симметричной криптосистемы** характерно применение одного и того же ключа как при шифровании, так и при расшифровании сообщений. В **асимметричных криптосистемах** для

зашифрования данных используется один (общедоступный) ключ, а для расшифрования – другой (секретный) ключ.

Симметричные криптосистемы

1. *Методы простой перестановки.*

Шифры перестановки

В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключем в данном случае является размеры таблицы. Например, сообщение “Неясное становится еще более непонятным” записывается в таблицу из 5 строк и 7 столбцов по столбцам.

Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

Для получения шифрованного сообщения текст считывается по строкам и группируется по 5 букв:

НОНСБ НЯЕЕО ЯОЕТЯ СВЕЛП НСТИЩ ЕОЫНА ТЕЕНМ

Несколько большей стойкостью к раскрытию обладает **метод одиночной перестановки** по ключу. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Используя в качестве ключа слово ЛУНАТИК, получим следующую таблицу:

Л	У	Н	А	Т	И	К			А	И	К	Л	Н	Т	У
4	7	5	1	6	2	3			1	2	3	4	5	6	7
Н	О	Н	С	Б	Н	Я			С	Н	Я	Н	Н	Б	О
Е	Е	О	Я	О	Е	Т			Я	Е	Т	Е	О	О	Е
Я	С	В	Е	Л	П	Н			Е	П	Н	Я	В	Л	С
С	Т	И	Щ	Е	О	Ы			Щ	О	Ы	С	И	Е	Т
Н	А	Т	Е	Е	Н	М			Е	Н	М	Н	Т	Е	А

До перестановки После перестановки

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если в ключе встретились бы одинаковые буквы, они бы нумеровались слева направо. Получается шифровка: СНЯНН БОЯЕТ ЕООЕЕ ПНЯВЛ СЩОЫС ИЕТЕН МНТЕА. Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

2. *Методы сложной перестановки.*

Кроме алгоритмов одиночных перестановок применяются **алгоритмы двойных перестановок**. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке порядок перестановок был обратный. Пример данного метода шифрования показан в следующих таблицах:

	2	4	1	3			1	2	3	4			1	2	3	4
4	П	Р	И	Е		4	И	П	Е	Р		1	А	З	Ю	Ж
1	З	Ж	А	Ю		1	А	З	Ю	Ж		2	Е	_	С	Ш

2	_	Ш	Е	С		2	Е.	_	С	Ш		З	Г	Т	О	О
З	Т	О	Г	О		З	Г	Т	О	О		4	И	П	Е	Р

Двойная перестановка столбцов и строк

В результате перестановки получена шифровка АЗЮЖЕ_СШГТООИПЕР. Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы.

Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3 х 3 их 36, для 4 х 4 их 576, а для 5*5 их 14400.

В средние века для шифрования применялись и **магические квадраты**. Магическими квадратами называются квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Для шифрования необходимо вписать исходный текст по приведенной в квадрате нумерации и затем переписать содержимое таблицы по строкам. В результате получается шифротекст, сформированный благодаря перестановке букв исходного сообщения.

16	3	2	13			О	И	Р	Т
5	10	11	8			З	Ш	Е	Ю
9	6	7	12			_	Ж	А	С
4	15	14	1			Е	Г	О	П

П Р И Е З Ж А Ю _ Ш Е С Т О Г О

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

Число магических квадратов очень резко возрастает с увеличением размера его сторон: для таблицы 3*3 таких квадратов -1; для таблицы 4*4 - 880; а для таблицы 5*5-250000.

3. Методы замены.

Шифры простой замены

Система шифрования Цезаря - частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на К букв.

Известная фраза Юлия Цезаря VENI VINI VICI – пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в SBKF SFAF SFZF (при смещении на 4 символа).

Греческим писателем Полибием за 100 лет до н.э. был изобретен так называемый **полибианский квадрат** размером 5*5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

Шифры сложной замены

Шифр Гронсфельда состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно также, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

Пусть в качестве ключа используется группа из трех цифр – 314, тогда

Сообщение СОВЕРШЕННО СЕКРЕТНО

Ключ 3143143143143143143

Шифровка ФПИСЬИОССАХИЛФИУСС

Устное повторение материала по вопросам:

1. Что такое криптография?
2. Что такое ключ?
3. Что такое криптоанализ?
4. Что такое кодирование?
5. Какова цель криптографического преобразования?
6. Перечислить основные алгоритмы шифрования

Примерные тесты

Тема 2. Основы информационной безопасности организации

1. Информационная война – это…

a. злословие в адрес другого человека;

b. информационное противоборство с целью нанесения ущерба важным структурам противника, подрыв его политической и социальной систем, а также дестабилизации общества и государства противника;

c. акт применения информационного оружия.

2. Информационная безопасность – это…

a. невозможность нанесения вреда свойствам объектам безопасности, обуславливаемым информацией и информационной инфраструктурой (защищенность от угроз);

b. предотвращение зла наносимого государственным структурам;

c. проведение природоохранных мероприятий.

3. К понятию информационной безопасности НЕ относятся:

a. природоохранные мероприятия;

b. надежность работы компьютера;

c. сохранность ценных данных.

4. К объектам информационной безопасности на предприятии НЕ относятся:

a. информационные ресурсы;

b. средства вычислительной и организационной техники;

c. Конституция России.

5. Обеспечение безопасности информации – это…

a. одноразовое мероприятие;

b. комплексное использование всего арсенала имеющихся средств защиты;

c. разработка каждой службой плановых мер по защите информации.

6. Третьим этапом построения системы защиты является:

a. планирование;

b. реализация;

c. анализ.

7. Какого подхода к обеспечению безопасности информации не существует?

a. комплексный;

b. фрагментарный;

c. теоретический.

8. Первым этапом построения системы защиты является:

a. анализ;

b. планирование;

c. сопровождение.

Зачетно-экзаменационные материалы для промежуточной аттестации (зачет)

Вопросы для подготовки к зачету

1. Понятие информационной безопасности. Основные составляющие информационной безопасности.
2. Проблема информационной безопасности на современном этапе.
3. Место информационной безопасности в системе национальной безопасности.
4. Роль информационной безопасности в обеспечении национальной безопасности государства.
5. Концептуальная модель информационной безопасности организации и основные понятия.
6. Система обеспечения информационной безопасности организации.
7. Направления защиты информации.
8. Способы защиты информации.
9. Классификация информации ограниченного доступа по видам тайны.
10. Понятие угрозы безопасности информации.
11. Общая классификация угроз.
12. Каналы несанкционированного доступа к конфиденциальной информации.
13. Методы несанкционированного доступа к конфиденциальной информации с использованием различных каналов.

14. Понятие комплексной системы защиты информации на предприятии.
15. Общая структура комплексной системы защиты информации на предприятии.
16. Компоненты комплексной системы защиты информации на предприятии.
17. Назначение комплексной системы защиты и ее стандартизация.
18. Правовые и организационные методы защиты информации.
19. Технические и программные методы защиты информации.
20. Классификация компьютерных вирусов.
21. Профилактика заражения и действия пользователя при заражении вирусами.
22. Зашифровать слово «книга», используя гамму 1001 в виде двоичного кода.
23. Зашифровать сообщение «Вопросы обеспечения защиты информации», используя шифр сложной перестановки и ключевое слово «привет».
24. Зашифровать сообщение «Вопросы обеспечения защиты информации», используя одноалфавитный шифр со сдвигом на 2 буквы.
25. Зашифровать сообщение «Вопросы обеспечения защиты информации», используя шифрование по диагонали.
26. Зашифровать сообщение «Вопросы обеспечения защиты информации», используя метод двойной перестановки с ключом «привет».
27. Зашифровать сообщение «Методы перестановки» с помощью ключа «зонд», используя матрицу Вижинера.
28. Зашифровать слово «защита» с использованием алгебры матриц с помощью ключа $A = \begin{pmatrix} 1 & 4 & 8 \\ 3 & 7 & 2 \\ 6 & 9 & 5 \end{pmatrix}$
29. Зашифровать сообщение «Информация первооснова деятельности людей», используя одноалфавитный шифр со сдвигом на 2 буквы.
30. Зашифровать сообщение «Информация имеет ценность», используя одноалфавитный шифр со сдвигом на 1 букву.
31. Зашифровать сообщение «Ценность информации изменяется во времени», используя шифрование по диагонали.

Критерии оценивания результатов обучения

«Зачтено» ставится студенту, который прочно усвоил предусмотренный программный материал; правильно, аргументировано ответил на все вопросы, с приведением примеров; показал глубокие систематизированные знания, владеет приемами рассуждения и сопоставляет материал из разных источников: теорию связывает с практикой, другими темами данного курса, других изучаемых предметов; без ошибок выполнил практическое задание. Обязательным условием выставленной оценки является правильная речь в быстром или умеренном темпе. Дополнительным условием получения оценки «зачтено» могут стать хорошие успехи при выполнении самостоятельной и контрольной работы, систематическая активная работа на семинарских (практических) занятиях.

«Не зачтено» ставится студенту, имеющему существенные пробелы в знании основного материала по программе, а также допустившему принципиальные ошибки при изложении материала.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на зачете;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,
– в форме электронного документа.
Для лиц с нарушениями слуха:
– в печатной форме,
– в форме электронного документа.
Для лиц с нарушениями опорно-двигательного аппарата:
– в печатной форме,
– в форме электронного документа.
Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5 ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ, ИНФОРМАЦИОННЫХ РЕСУРСОВ И ТЕХНОЛОГИЙ

5.1 Учебная литература

1. Внуков, А. А. Защита информации в банковских системах: учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2021. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/468273

2. Внуков, А. А. Защита информации: учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2021. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/470131

3. Зенков, А. В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. — Москва: Издательство Юрайт, 2021. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/477968

4. Корабельников, С. М. Преступления в сфере информационной безопасности: учебное пособие для вузов / С. М. Корабельников. — Москва: Издательство Юрайт, 2021. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/476798

5. Кузнецова, Е. И. Экономическая безопасность: учебник и практикум для вузов / Е. И. Кузнецова. — 2-е изд. — Москва: Издательство Юрайт, 2021. — 336 с. — (Высшее образование). — ISBN 978-5-534-14514-4. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/477803 (дата обращения: 30.06.2021).

6. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2021. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469235 (дата обращения: 16.08.2021).

7. Рассолов, И. М. Информационное право: учебник и практикум для вузов / И. М. Рассолов. — 6-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2021. — 415 с. — (Высшее образование). — ISBN 978-5-534-14327-0. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/479850

8. Суворова, Г. М. Информационная безопасность: учебное пособие для вузов / Г. М. Суворова. — Москва: Издательство Юрайт, 2021. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/467370

9. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты: учебник для вузов / В. М. Фомичёв, Д. А. Мельников; под редакцией В. М. Фомичёва. — Москва: Издательство Юрайт, 2021. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469567

10. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты: учебник для вузов / В. М. Фомичёв, Д. А. Мельников; под редакцией В. М. Фомичёва. — Москва: Издательство Юрайт, 2021. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/470279

11. Экономическая безопасность: учебник для вузов / Л. П. Гончаренко [и др.] ; под общей редакцией Л. П. Гончаренко. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2021. — 340 с. — (Высшее образование). — ISBN 978-5-534-06090-4. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/469005 (дата обращения: 30.06.2021).

12. Экономическая информатика: учебник и практикум для бакалавриата и магистратуры / Ю. Д. Романова [и др.] ; ответственный редактор Ю. Д. Романова. — Москва: Издательство Юрайт, 2019. — 495 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-9916-3770-1. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/426110

5.2 Периодическая литература

1. Журнал “Архитектура и современные информационные технологии» - http://www.marhi.ru/AMIT
2. Журнал «Информационные технологии и общество» - http://ifets.ieee.org/russian/periodical/journal.html
3. Журнал «Компьютерра» - http://www.computerra.ru
4. Журнал «Программные продукты и системы» - http://swsys.ru
5. Журнал «Мир ПК» - http://www.osp.ru/pcworld/#/home
6. Журнал «Сети» - http://www.osp.ru/nets/#/home
7. Электронные журналы по информатике - www.osp.ru
8. Журнал «Бизнес-информатика» - http://bijournal.hse.ru

5.3 Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронно-библиотечные системы (ЭБС):

1. ЭБС «ЮРАЙТ». - URL: https://urait.ru/
2. ЭБС «УНИВЕРСИТЕТСКАЯ БИБЛИОТЕКА ОНЛАЙН». - URL: www.biblioclub.ru
3. ЭБС «ZNANIUM.COM». - URL: www.znanium.com
4. ЭБС «ЛАНЬ». - URL: https://e.lanbook.com

Профессиональные базы данных:

1. Университетская информационная система РОССИЯ http://uisrussia.msu.ru
2. Научная электронная библиотека (НЭБ) http://www.elibrary.ru/

Информационные справочные системы:

1. Справочно-правовая система «Консультант Плюс» (http://www.consultant.ru).
2. Информационно-правовая система «Гарант» (http://www.garant.ru или доступ по локальной сети с компьютеров библиотеки)

Ресурсы свободного доступа:

1. КиберЛенинка (http://cyberleninka.ru/);
2. Словари и энциклопедии http://dic.academic.ru/.

Собственные электронные образовательные и информационные ресурсы КубГУ:

1. База учебных планов, учебно-методических комплексов, публикаций и конференций. URL: http://mschool.kubsu.ru/
2. Электронная библиотека НБ КубГУ (Электронный каталог). - URL:http://megapro.kubsu.ru/MegaPro/Web

6 МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При изучении дисциплины используются следующие формы работы.

1. Лекции, на которых рассматриваются основные теоретические вопросы данной дисциплины. Лекции проводятся в следующих формах: лекция.

2. Лабораторные занятия, на которых выполняются практические упражнения с применением технических средств, заслушиваются рефераты, проводится тестирование. При подготовке к лабораторному занятию следует:

- использовать рекомендованные преподавателями учебники и учебные пособия - для закрепления теоретического материала;

- разобрать совместно с другими студентами и обсудить вопросы по теме лабораторного занятия и т.д.

3. Самостоятельная работа, которая является одним из главных методов изучения дисциплины.

Цель самостоятельной работы – расширение кругозора и углубление знаний в области теории и практики вопросов изучаемой дисциплины.

Контроль за выполнением самостоятельной работы проводится при изучении каждой темы дисциплины на лабораторных занятиях. Это текущий опрос, подготовка рефератов, тестовые задания.

Самостоятельная работа студента в процессе освоения дисциплины включает в себя:

– изучение основной и дополнительной литературы по курсу;

– работу с электронными библиотечными системами;

– изучение материалов периодической печати, Интернет - ресурсов;

– выполнение рефератов;

– индивидуальные и групповые консультации;

– подготовку к зачету.

4. Зачет по дисциплине. Зачет сдаётся в устной форме. Представляет собой структурированное задание по всем разделам дисциплины. Для подготовки следует воспользоваться рекомендованным преподавателем учебниками, методическими указаниями к практическим занятиям и самостоятельной контролируемой работе студента по дисциплине, глоссарием, своими конспектами лекций и практических занятий, выполненными самостоятельными работами.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

7 МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПО ДИСЦИПЛИНЕ

Наименование специальных помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации 352120, Краснодарский край, г. Тихорецк, ул. Октябрьская, д. 24б, № 303	Мультимедийный проектор, персональный компьютер, выход в Интернет, электронные ресурсы, экран, учебная мебель, доска учебная, учебно-наглядные пособия, обеспечивающие тематические иллюстрации
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации 352120, Краснодарский край, г. Тихорецк, ул. Октябрьская, д. 24б, № 404	Мультимедийный проектор, персональный компьютер, экран, выход в Интернет, электронные ресурсы, учебная мебель, доска учебная, учебно-наглядные пособия, обеспечивающие тематические иллюстрации
Помещение для самостоятельной работы, с рабочими местами, оснащенными компьютерной техникой с подключением к сети «Интернет» и обеспечением неограниченного	Персональные компьютеры, принтер, выход в Интернет, учебная мебель

доступа в электронную информационно-образовательную среду организации для каждого обучающегося 352120, Краснодарский край, г. Тихорецк, ул. Октябрьская, д. 24б № 406	
Помещение для самостоятельной работы, с рабочими местами, оснащенными компьютерной техникой с подключением к сети «Интернет» и обеспечением неограниченного доступа в электронную информационно-образовательную среду организации для каждого обучающегося, в соответствии с объемом изучаемых дисциплин 352120, Краснодарский край, г. Тихорецк, ул. Октябрьская, д. 24б, № 36	Персональные компьютеры, принтер, выход в Интернет, учебная мебель
Помещение для хранения и профилактического обслуживания учебного оборудования 352120, Краснодарский край, г. Тихорецк, ул. Октябрьская, д. 24б № 99 а	Стол компьютерный, сейф, мебель офисная, стеллажи металлические