МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Экономический факультет

УТВЕРЖДАЮ:
Проректор по учебной работе,
качеству образования – первый
проректор
_____ Т.А. Хагуров
подпись
«25» мая 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.22 Криптография и информационная безопасность
(код и наименование дисциплины в соответствии с учебным планом)

Направление подготовки: 27.03.03 Системный анализ и управление
(код и наименование направления подготовки/специальности)

Направленность (профиль):
Интеллектуальная бизнес-аналитика и управление экономическими процессами
(наименование направленности (профиля) / специализации)

Форма обучения: _____очная_____
(очная, очно-заочная, заочная)

Квалификация: бакалавр

Краснодар 2022

Рабочая программа дисциплины Б1.В.22 Криптография и информационная безопасность составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 27.03.03 Системный анализ и управление.
(код и наименование направления подготовки)

Программу составил:
Т.В. Васкевич, старший преподаватель,
кандидат педагогических наук _____
И.О. Фамилия, должность, ученая степень, ученое звание подпись

Рабочая программа дисциплины Б1.В.22 Криптография и информационная безопасность утверждена на заседании кафедры экономики и управления инновационными системами
протокол №5 от «11» мая 2022 г.
Заведующий кафедрой экономики
и управления инновационными системами Литвинский К.О._____
фамилия, инициалы подпись

Утверждена на заседании учебно-методической комиссии экономического факультета протокол № 11 от «17» мая 2022 г.
Председатель УМК факультета Дробышевская Л.Н. _____
фамилия, инициалы подпись

Рецензенты:
Качанова Ирина Александровна, доцент кафедры математических и компьютерных методов ФГБОУ ВО «Кубанский государственный университет», кандидат физико-математических наук

Силюк В.А., генеральный директор, ООО «Акпром»

1 Цели и задачи изучения дисциплины (модуля)

1.1 Цель освоения дисциплины

Цель – формирование у бакалавров знаний в области теоретических основ информационной безопасности и криптографии; навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах.

1.2 Задачи дисциплины

– изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах;

– изучение процессов обеспечения информационной безопасности на основе инструментария криптографии

– овладение инструментарием работы с программным обеспечением для практического освоения принципов и методов защиты экономической информации;

– формирование комплексных знаний об основных тенденциях развития технологий защиты информации, об уровнях организации и реализации информационной защиты;

– формирование навыков обеспечения защиты объектов интеллектуальной собственности и результатов исследований и разработок как коммерческой тайны предприятия.

1.3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Криптография и информационная безопасность» относится к части, формируемой участниками образовательных отношений Блока 1 "Дисциплины (модули)" учебного плана. В соответствии с рабочим учебным планом дисциплина изучается на 4 курсе по очной форме обучения. Вид промежуточной аттестации: зачет.

Дисциплина формируется на основе изучения дисциплины «Информатика», «Базы данных», «Методы сбора и систематизации информации», «Информационно-аналитическая инфраструктура». Последующие дисциплины, для которых данная дисциплина является предшествующей в соответствии с учебным планом: «Методы и средства проектирования информационных систем».

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

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине
ПК-1 Способен управлять ресурсами информационных технологий при решении задач профессиональной деятельности	
ИПК-1.4 Оценивает и управляет процессами обеспечения информационной безопасности, в т.ч. на основе инструментария криптографии	Знает основы информационной безопасности и защиты информации
	Знает типовые разработанные средства защиты информации и возможности их использования в реальных задачах создания и внедрения информационных систем
	Знает принципы криптографических преобразований, типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа
	Умеет проводить анализ степени защищенности информации и осуществлять повышение уровня защиты с учетом развития математического и программного обеспечения вычислительных систем
	Умеет формулировать требования к шифрам и основные характеристики шифров

Код и наименование индикатора* достижения компетенции	Результаты обучения по дисциплине
	пользоваться криптографической терминологией
	Имеет навыки в реализации мероприятий по обеспечению на предприятии (в организации) деятельности в области защиты информации
	Владеет навыками использования основных типов шифров и криптографических алгоритмов

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 зачетных единиц (72 часа), их распределение по видам работ представлено в таблице

Виды работ		Всего часов	Форма обучения			
			очная		очно-заочная	заочная
			7 семестр (часы)	X семестр (часы)	X семестр (часы)	X курс (часы)
Контактная работа, в том числе:		**38,2**	**38,2**			
Аудиторные занятия (всего):		**34**	**34**			
занятия лекционного типа		18	18			
лабораторные занятия		16	16			
практические занятия						
семинарские занятия						
Иная контактная работа:						
Контроль самостоятельной работы (КСР)		4	4			
Промежуточная аттестация (ИКР)		0,2	0,2			
Самостоятельная работа, в том числе:		**33,8**	**33,8**			
Выполнение индивидуальных заданий (подготовка сообщений, презентаций, подготовка к тестированию, контрольная работа)		20	20			
Реферат (подготовка)		10	10			
Самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям)		3,8	3,8			
Контроль:						
Подготовка к экзамену						
Общая трудоемкость	**час.**	**72**	**72**			
	в том числе контактная работа	**38,2**	**38,2**			
	зач. ед	**2**	**2**			

2.2 Содержание дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы (темы) дисциплины, изучаемые в 7 семестре *(очная форма обучения)*

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Внеаудиторная работа
			Л	ПЗ	ЛР	СРС
1.	Введение в информационную безопасность	7	2			5
2.	Правовое обеспечение информационной безопасности	7	2			5
3.	Организационное обеспечение информационной безопасности	11	2		4	5
4.	Технические средства и методы защиты информации.	13	4			5
5.	Программно-аппаратные средства и методы обеспечения информационной безопасности	13	4		8	5
6.	Криптографические методы защиты информации	16,8	4		4	8,8
	ИТОГО по разделам дисциплины	67,8	18		16	33,8
	Контроль самостоятельной работы (КСР)	4				4
	Промежуточная аттестация (ИКР)	0,2				0,2
	Подготовка к текущему контролю					
	Общая трудоемкость по дисциплине	72	18		16	38

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

2.3 Содержание разделов (тем) дисциплины

2.3.1 Занятия лекционного типа

№	Наименование раздела (темы)	Содержание раздела (темы)	Форма текущего контроля
1.	Введение в информационную безопасность	Понятие и виды угроз информационной безопасности бизнеса. Политика безопасности. Виды информационных угроз и защита от них. Цифровые сертификаты. Алгоритмические и организационные методы защиты. Цифровая подпись. Модели информационной безопасности. Биометрия. Информационная война. Информационный терроризм.	Тесты для актуализации и проверки знаний, опрос, реферат
2.	Правовое обеспечение информационной безопасности	Основные нормативно-правовые акты в области информационной безопасности. Правовые особенности обеспечения безопасности конфиденциальной информации и государственной тайны. Доктрина информационной безопасности РФ. Законодательный уровень защиты информации.	Тесты для актуализации и проверки знаний, опрос, реферат
3.	Организационное обеспечение информационной безопасности	Основные стандарты в области обеспечения информационной безопасности. Политика безопасности. Экономическая безопасность предприятия. Процедурный уровень обеспечения информационной безопасности. Индивидуальная и государственная защита информации.	Тесты для актуализации и проверки знаний, собеседование, опрос, реферат
4.	Технические средства и методы защиты информации.	Инженерная защита объектов. Защита информации от утечки по техническим каналам. Технические средства негласного съема информации. Способы защиты информации. Активное и пассивное техническое средство защиты.	Тесты для актуализации и проверки знаний, опрос, реферат
5.	Программно-аппаратные средства и методы обеспечения информационной безопасности	Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз. Компьютерные вирусы и антивирусные программы. Методы и технологии борьбы с компьютерными вирусами.	Тесты для актуализации и проверки знаний, опрос, реферат

6.	Криптографические методы защиты информации	Симметричные и ассиметричные системы шифрования. Цифровые подписи (Электронные подписи). Инфраструктура открытых ключей. Криптографические протоколы.	Тесты для актуализации и проверки знаний, опрос, реферат

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

№	Наименование раздела (темы)	Тематика занятий/работ	Форма текущего контроля
1.	Организационное обеспечение информационной безопасности	Применение информационных технологий для изучения вопросов организационно-правового обеспечения информационной безопасности. Использование баз данных для нахождения и изучения нормативных документов в области информационной безопасности.	Решение практико-ориентированных задач на компьютере, опрос
2.	Программно-аппаратные средства и методы обеспечения информационной безопасности	Реализация работы инфраструктуры открытых ключей. Создание удостоверяющего центра, генерация открытых и секретных ключей, создание сертификатов открытых ключей, создание электронной подписи, проверка электронной подписи. Создание защищенного канала связи средствами виртуальной частной сети. Изучение настроек средств антивирусной защиты информации.	Решение практико-ориентированных задач на компьютере, опрос
3.	Криптографические методы защиты информации	Использование криптографических средств защиты информации Создание зашифрованных файлов и криптоконтейнеров и их расшифрование. Использование средств стеганографии для защиты файлов. Формы и методы проведения занятий по теме, применяемые образовательные технологии:	Контрольная работа на компьютере, решение практико-ориентированных задач на компьютере, опрос

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т) и т.д.

2.3.3 Примерная тематика курсовых работ (проектов)

Не предусмотрено

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

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	Занятия лекционного и лабораторного типа	Методические указания для подготовки к занятиям лекционного и семинарского типа. Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ». Протокол № 1 от 30 августа 2018 года. Режим доступа: https://www.kubsu.ru/ru/econ/metodicheskie-ukazaniya
2	Выполнение самостоятельной работы обучающихся	Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ». Протокол № 1 от 30 августа 2018 года. Режим доступа: https://www.kubsu.ru/ru/econ/metodicheskie-ukazaniya
3	Подготовка эссе, рефератов	Методические указания для подготовки эссе, рефератов, курсовых работ. Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ». Протокол № 1 от 30 августа 2018 года. Режим доступа:https://www.kubsu.ru/ru/econ/metodicheskie-ukazaniya
4	Интерактивные методы	Методические указания по интерактивным методам обучения.

	обучения	Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ». Протокол № 1 от 30 августа 2018 года. Режим доступа: https://www.kubsu.ru/ru/econ/metodicheskie-ukazaniya

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 (модуля)

В ходе изучения дисциплины предусмотрено использование следующих образовательных технологий: лекции (аудиторные занятия в форме лекций с использованием комплекта мультимедийного оборудования, в т.ч. интерактивная доска, компьютеры и пр.), лабораторные занятия, проблемное обучение, модульная технология, анализ практических ситуаций, решений бизнес-кейсов, подготовка письменных аналитических работ, самостоятельная работа студентов.

Компетентностный подход в рамках преподавания дисциплины реализуется в использовании интерактивных технологий и активных методов (проектных методик, мозгового штурма, разбора конкретных ситуаций,) в сочетании с внеаудиторной работой.

Информационные технологии, применяемые при изучении дисциплины: использование информационных ресурсов, доступных в информационно-телекоммуникационной сети Интернет. Самостоятельная работа проводится с использованием библиотеки и посредством сети Интернет.

В целях реализации рабочей программы для инвалидов и ЛОВЗ применяются специализированные технические средства приема-передачи учебной информации в доступных формах для обучающихся с различными нарушениями, обеспечивается выпуск альтернативных форматов печатных материалов (крупный шрифт), электронных образовательных ресурсов в формах, адаптированных к ограничениям здоровья обучающихся, наличие необходимого материально-технического оснащения.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием информационно-образовательной среды ВУЗа.

7. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «Криптография и информационная безопасность».

Оценочные средства включает контрольные материалы для проведения **текущего контроля** в форме тестовых заданий, доклада-презентации по проблемным вопросам, разноуровневых заданий, ситуационных задач и **промежуточной аттестации** в форме вопросов и заданий к зачету.

Структура оценочных средств для текущей и промежуточной аттестации

№ 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	ИПК-1.4 Оценивает и управляет процессами обеспечения информационной безопасности, в т.ч. на основе инструментария криптографии	Знает основы информационной безопасности и защиты информации; знает типовые разработанные средства защиты информации и возможности их использования в реальных задачах создания и внедрения информационных систем; знает принципы криптографических преобразований, типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа; Умеет проводить анализ степени защищенности информации и осуществлять повышение уровня защиты с учетом развития математического и программного обеспечения вычислительных систем; умеет формулировать требования к шифрам и основные характеристики шифров пользоваться криптографической терминологией; Имеет навыки в реализации мероприятий по обеспечению на предприятии (в организации) деятельности в области защиты информации; Владеет навыками использования основных типов шифров и криптографических алгоритмов	Контрольные работы на компьютере, практико-ориентированные задачи на компьютере, проверочные тесты, вопросы для устного опроса, рефераты	Вопрос на зачете 1-27

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

Примерный перечень аналитических заданий для проведения устных опросов

1. Что такое информационная безопасность?
2. Перечислите основные угрозы информационной безопасности.
3. Какие существуют модели информационной безопасности?
4. Какие методы защиты информации выделяют?
5. Что такое правовые методы защиты информации?

6. Что такое организационные методы защиты информации?
7. Что такое технические методы защиты информации?
8. Что такое программно-аппаратные методы защиты информации?
9. Что такое криптографические методы защиты информации?
10. Что такое физические методы защиты информации?
11. Какие главные государственные органы в области обеспечения информационной безопасности?
12. Перечислите виды защищаемой информации.
13. Правовое обеспечение информационной безопасности
14. Какие основные законы в области защиты информации в РФ?
15. Перечислите основные цели и задачи РФ в области обеспечения информационной безопасности
16. Что такое концепция информационной безопасности?
17. Что такое конфиденциальная информация?
18. Что такое персональные данные?
19. В каких случаях возможно использовать персональные данные без согласия обладателя?
20. Охарактеризуйте биометрические данные как персональные данные.
21. Что такое профессиональная тайна?
22. Что такое коммерческая тайна?
23. Что такое режим коммерческой тайны?
24. Что такое государственная тайна?
25. Опишите правовой режим государственной тайны.
26. Какие государственные органы занимаются сертификацией и лицензированием средств защиты информации?
27. Организационное обеспечение информационной безопасности
28. Какие основные международные стандарты в области информационной безопасности существуют?
29. Что такое "Единые критерии"
30. Как связаны международные стандарты и стандарты РФ?
31. Какие основные стандарты РФ в области информационной безопасности существуют?
32. Охарактеризуйте стандарт ГОСТ Р ИСО/МЭК 27002-2014.
33. Что такое политика безопасности?
34. Какое количество средств бюджета организации эффективно тратить для обеспечения информационной безопасности?
35. Технические средства и методы защиты информации
36. Что такое инженерная защита объектов?
37. Какие виды сигнализаций устанавливаются для обеспечения инженерной защиты?
38. Что такое технические каналы утечки информации?
39. Перечислите основные виды технических каналов утечки информации?
40. Перечислите методы защиты информации от утечки по визуальному каналу.
41. Перечислите методы защиты информации от утечки по воздушному каналу.
42. Перечислите методы защиты информации от утечки по вибрационному каналу.
43. Перечислите методы защиты информации от утечки по индукционному каналу.
44. Перечислите средства и методы защиты информации от утечки в телефонных линиях.
45. Перечислите основные мероприятия по обеспечению защиты информации от утечки по техническим каналам.
46. Какие виды компьютерных угроз существуют?
47. Что такое брандмауэр?
48. Что такое антивирусная программа?

49. Что такое эвристический алгоритм поиска вирусов?
50. Что такое сигнатурный поиск вирусов?
51. Методы противодействия сниффингу?
52. Какие программные реализации программно-аппаратных средств защиты информации вы знаете?
53. Что такое механизм контроля и разграничения доступа?
54. Какую роль несет журналирование действий в программно-аппаратных средствах защиты информации?
55. Что такое средства стеганографической защиты информации?
56. Что такое криптография?
57. Какие используются симметричные алгоритмы шифрования?
58. Какие используются ассиметричные алгоритмы шифрования?
59. Что такое криптографическая хеш-функция?
60. Какие используются криптографические хеш-функции?
61. Что такое цифровая подпись?
62. Что такое инфраструктура открытых ключей?
63. Какие российские и международные стандарты на формирование цифровой подписи существуют?
64. Какие основные криптографические протоколы используются в сетях?

Контрольная работа на компьютере по теме «Использование классических криптоалгоритмов подстановки и перестановки для защиты информации»

Цель работы: Изучение классических криптографических алгоритмов моноалфавитной подстановки, многоалфавитной подстановки и перестановки для защиты информации. Использование гистограмм, отображающих частоту встречаемости символов в тексте для криптоанализа классических шифров.

Для выполнения работы необходимо запустить программу L_LUX.EXE.

На экране дисплея появляется окно, с размещенным в его центре текстовым редактором (для отображения зашифрованных и расшифрованных текстов), в верхней строке окна расположено главное меню, позволяющее пользователю выполнить требуемое действие, чуть ниже основного меню расположена панель инструментов (для управления быстрыми командными кнопками и другими “горячими” элементами управления), а в самом низу окна, под текстовым редактором, находится строка состояния, в которой указывается подсказка и выводится дополнительная информация. Клавиши панели инструментов, для удобства, снабжены всплывающими подсказками. Для того чтобы попасть в основное меню, необходимо нажать клавишу F10. Передвижение по главному меню осуществляется клавишами перемещения курсора. Чтобы вызвать пункт меню, нужно нажать клавишу “ENTER”, вернуться в главное меню или вовсе выйти из него – “ESC”.

1.1. Редактор. Данный пункт основного меню содержит подпункты: создать документ, открыть файл, сохранить файл, выход из программы. Предварительно, сразу после запуска программы, текстовый редактор недоступен, также недоступными являются почти все пункты главного меню (кроме создания документа, открытия файла, выхода из программы, информации о программе) и большая часть клавиш панели управления (за исключением создания документа, открытия файла и выхода из программы).

Создать документ (Ctrl+N) – данный подпункт делает доступным для работы тестовый редактор (пользователь получает право создать свой текстовый файл, который впоследствии можно будет использовать при работе с программой), также появляется возможность использовать все недоступные до этого пункты основного меню и клавиши панели управления.

Открыть файл (Ctrl+L) – при выборе этого пункта появляется диалоговое окно, предоставляющее возможность выбора файла для загрузки. При этом содержимое файла будет отображено в окне редактора текстов. Аналогично пункту “Создать документ” доступным для работы становится текстовый редактор с отображаемым текстом, а также появляется возможность использовать все недоступные до этого пункты основного меню и клавиши панели управления. Сохранить файл (Ctrl+S) - при выборе этого пункта появляется диалоговое окно, позволяющее сохранить на диск содержимое редактора текстов. Выход из программы (Ctrl+X) – при выборе этого пункта появляется диалоговое окно, позволяющее выйти из программы.

1.2. Гистограмма. Вывод на экран двух гистограмм, отображающих частоту встречаемости символов в тексте. До выполнения шифрования и дешифрования вызывать гистограмму не имеет смысла, так как еще не сформированы тексты, для которых будет просматриваться гистограмма. Имеется возможность просмотра следующих сочетаний гистограмм: гистограммы исходного и зашифрованного файла, гистограммы зашифрованного и расшифрованного файла, гистограммы стандартного распределения и зашифрованного текста, гистограммы стандартного распределения и расшифрованного текста.

1.3. Шифрование. Выполнение шифрования текстового файла осуществляется из семи методов, рассматриваемых в контрольной работе.

1. Одноалфавитный метод (с фиксированным смещением).
2. Одноалфавитный метод с задаваемым смещением (от 2 до 20).
3. Перестановка символов.
4. По дополнению до 255 (инверсный метод).
5. Многоалфавитный метод (с фиксированным ключом).
6. Многоалфавитный метод с ключом фиксированной длины. 7. Многоалфавитный метод с ключом произвольной длины.

Выбор метода шифрования производится как мышкой, так и клавишами перемещения курсора и клавишей “ENTER”.

Затем появляется окно в котором в зависимости от метода шифрования требуется указать те или иные параметры, и либо подтвердить процесс кодировки, либо отказаться от него.

1.4. Расшифрование. Аналогично предыдущему пункту выбирается метод расшифрования (должен соответствовать методу, которым был зашифрован файл). Снова появляется окно, в котором в зависимости от метода расшифрования требуется указать те или иные параметры, и либо подтвердить процесс расшифрования, либо отказаться от него. После этого в окно редактора будет выдан расшифрованный текст. При правильном расшифровании, полученный текст совпадает с исходным.

1.5. Дополнительная информация. Программа предусматривает возможность посмотреть дополнительную информацию.

Пример работы с программой. В качестве примера рассмотрим одноалфавитное шифрование с фиксированным ключом.

Нажав клавиши Ctrl+L, либо выбрав в меню пункт «Открыть файл», загрузите в окно редактора исходный текст. Затем вызовите пункт меню «Шифрование», выберите одноалфавитный метод (с фиксированным смещением). В появившемся окне нажмите клавишу «Зашифровать». После того, как шифрование выполнено, можно также просмотреть в редакторе зашифрованный текст.

Перейдите к пункту меню «Гистограмма». Выберите тип гистограмм, отображающий гистограммы исходного и шифрованного файлов. Проанализируйте гистограммы. Они должны иметь примерно одинаковый вид. Чтобы узнать ключ шифра, (смещение второго алфавита относительно первого), необходимо найти по гистограммам символы, имеющие одинаковую частоту встречаемости. Например, самый частый символ в первой

гистограмме при шифровании должен перейти в самый частый символ во второй гистограмме.

Таким образом, найдя два самых часто встречаемых символа в обеих гистограммах, можно по стандартной таблице ASCII кодов вычислить смещение. Зная смещение и таблицу кодировки символов, текст можно легко расшифровать. Вызвав пункт меню

«Дешифрование», можно провести те же действия в автоматическом режиме.

Задание:

Для одноалфавитного метода с фиксированным смещением определит установленное в программе смещение. Для этого: просмотреть предварительно созданный с помощью редактора свой текстовый файл; выполнить для этого файла шифрование; просмотреть в редакторе зашифрованный файл; просмотреть гистограммы исходного и зашифрованного текстов, описать гистограммы (в чем похожи, чем отличаются) и определить, с каким смещением было выполнено шифрование; расшифровать зашифрованный текст:

1) с помощью программы, после чего проверить в редакторе правильность расшифрования;

2) вручную с помощью гистограмм; описать и объяснить процесс дешифрования.

В отчете для каждого метода шифрования описывается последовательность выполняемых действий, имена всех использованных файлов, описываются полученные гистограммы, указывается найденное смещение, описывается процесс дешифрования.

Преподавателю предоставляется отчет о проделанной работе и все использованные и созданные файлы.

Для одноалфавитного метода с задаваемым смещением (шифр Цезаря): для своего исходного текста выполнить шифрование с произвольным смещением; просмотреть и описать гистограммы исходного и зашифрованного текстов, определить смещение для нескольких символов; расшифровать текст с помощью программы; имеется зашифрованный шифром Цезаря текст; дешифровать его с помощью программы методом подбора смещения; указать, с каким смещением был зашифрован файл.

Для метода перестановки символов дешифровать зашифрованный файл. Для этого необходимо определить закон перестановки символов открытого текста. Создайте небольшой файл длиной в несколько слов с известным вам текстом, зашифруйте его, просмотрите гистограммы (опишите их; ответьте, можно ли извлечь из них полезную для дешифрации информацию). Сравните (с помощью редактора) ваш исходный и зашифрованный тексты и определите закон перестановки символов.

Дешифруйте файл:

1) вручную (объясните ваши действия);

2) с помощью программы.

Для инверсного кодирования (по дополнению до 255): для своего произвольного файла выполните шифрование; просмотрите гистограммы исходного и зашифрованного текстов, опишите гистограммы и определите смещение для нескольких символов; дешифруйте зашифрованный текст, проверьте в редакторе правильность дешифрования.

Для многоалфавитного шифрования с фиксированным ключом определите, сколько одноалфавитных методов и с каким смещением используется в программе. Для этого нужно создать свой файл, состоящий из строки одинаковых символов, выполнить для него шифрование и по гистограмме определить способ шифрования и набор смещений.

Для многоалфавитного шифрования с ключом фиксированной длины: для файла, состоящего из строки одинаковых символов выполнить шифрование и определить по гистограмме, какое смещение получает каждый символ; для файла произвольного текста произвести шифрование и расшифрование; просмотреть и описать гистограммы исходного и зашифрованного текстов; ответить, какую информацию можно получить из гистограмм.

Для многоалфавитного шифрования с произвольным паролем задание полностью аналогично. Привести в отчете ответы на контрольные вопросы, в соответствии с номером варианта, указанным преподавателем.

Номер варианта	**Контрольные вопросы**
1, 5, 7, 3, 9, 18, 28	Какие вы знаете методы криптографической защиты файлов? Чем отличается “псевдооткрытый” текст (текст, полученный при расшифровке по ложному ключу) от настоящего открытого текста?
2, 4, 6, 8, 20, 22, 24, 26,30	В чем преимущества и недостатки одноалфавитных методов? Как зависит время вскрытия шифра описанным выше способом подбора ключей от длины “вероятного” слова?
11, 13, 15, 10, 17,19, 27	Если вам необходимо зашифровать текст, содержащий важную информацию, какой метод, из рассмотренных, вы выберете? Обоснуйте свой выбор. Зависит ли время вскрытия шифра гаммирования (или таблицы Виженера) от мощности алфавита гаммы?
12, 14, 16, 21, 23, 25, 29	Целесообразно ли повторно применять для уже зашифрованного текста: а) метод многоалфавитного шифрования? б) метод Цезаря? В чем недостатки метода дешифрования с использованием протяжки вероятного слова?

Практико-ориентированная задача на компьютере «Изучение программных продуктов защиты информации. Программа PGP (Pretty Good Privacy)

Цель работы: Ознакомление с общими принципами построения и использования программных средств защиты информации, в частности с программой PGP.

Освоение средств программной системы PGP, предназначенных для:

- шифрования конфиденциальных ресурсов и разграничения доступа к ним;
- обеспечения целостности информационных ресурсов с помощью механизма электронной цифровой подписи;
- надежного уничтожения остаточной конфиденциальной информации;
- скрытия присутствия в компьютерной системе конфиденциальной информации с помощью виртуального диска.

Практико-ориентированная задача на компьютере «Анализ рисков информационной безопасности при организации защищенного документооборота в организации»

Цель работы: Ознакомление с современными методами анализа и управления рисками информационной безопасности. Получение практических навыков использования программного инструментария для анализа рисков информационной безопасности (на примере программы CORAS).

Реферат

Примерная тематика рефератов:

1. Информационная безопасность и информационная война.
2. Современные проблемы обеспечения безопасности информации.
3. Организация защиты коммерческой информации.
4. Средства массовой информации и безопасность.
5. Государственная и индивидуальная защита информации.
6. Обеспечение режима секретности.
7. Организация защиты коммерческой информации.
8. Методы борьбы с компьютерными вирусами.
9. Реклама как источник информационной опасности.
10. Компьютерные вирусы и хакерские атаки.
11. Криптография как одна из базовых технологий безопасности операционных систем.
12. Виды шифрования.
13. Принципы защищенного электронного документооборота в телекоммуникационных сетях и алгоритмами постановки электронной подписи.

Примерные варианты тестов для текущей аттестации:

Вариант 1

1. Программа, которая может размножаться, присоединяя свой код к другой программе, называется

Выберите один ответ.

a. Компилятор
b. Интернет-черви
c. Вирус

2. **Величиной (размером) ущерба (вреда), ожидаемого в результате несанкционированного доступа к информации или нарушения доступности информационной системы, называется**

Выберите один ответ.

a. Воздействием (влиянием)
b. Потерей
c. Силой

3. Код, способный самостоятельно, то есть без внедрения в другие программы, вызвать распространение своих копий по информационной системе и их выполнение, называется

Выберите один ответ.

a. Троянской программой
b. Червем
c. Вирусом

4. Уровень риска, который считается доступным для достижения желаемого результата, называется

Выберите один ответ.

a. Устойчивостью
b. Терпимостью по отношению к риску
c. Независимостью

5. Компьютер с одним процессором в каждый конкретный момент времени может выполнять команд

Выберите один ответ.

a. Две

b. Одну
c. Сколько зададут

6. Алгоритмы реального времени, заранее назначающие каждому процессу фиксированный приоритет, после чего выполняющие приоритетное планирование с переключениями, называются:

Выберите один ответ.
a. Статическими алгоритмами
b. Алгоритмы RMS
c. Динамическими алгоритмами

7. Системные файлы, обеспечивающие поддержку структур файловой системы, называются:

Выберите один ответ.
a. Каталоги
b. Символьные файлы
c. Регулярные файлы

8. Коды, обладающие способностью к распространению (возможно, с изменениями) путем внедрения в другие программы, называются

Выберите один ответ.
a. Вирусами
b. Руткитами
c. Червями

9. Требованием к информационной системе, являющимся следствием действующего законодательства, миссии и потребностей организации, называется:

Выберите один ответ.
a. Правилами безопасности
b. Требованием безопасности
c. Мерами безопасности

10. Процессом идентификации рисков применительно к безопасности информационной системы, определения вероятности их осуществления и потенциального воздействия, а также дополнительный контрмер, ослабляющий (уменьшающий) это воздействие, называется:

Выберите один ответ.
a. Управление риском
b. Предупреждением рисков
c. Анализом рисков

11. Компьютерная система, в которой два или более центральных процессоров делят полный доступ к общей оперативной памяти, называется

Выберите один ответ.
a. Мультипроцессоры типа «хозяин-подчиненный»
b. Симметричный мультипроцессор
c. Мультипроцессор с общей памятью

12. К правовым методам, обеспечивающим информационную безопасность, относятся:

Выберите один ответ.
a. Разработка аппаратных средств обеспечения правовых данных
b. Разработка и установка во всех компьютерных правовых сетях журналов учета действий
c. Разработка и конкретизация правовых нормативных актов обеспечения безопасности

13. Основными источниками угроз информационной безопасности являются все указанное в списке:

Выберите один ответ.

a. Хищение жестких дисков, подключение к сети, инсайдерство
b. Перехват данных, хищение данных, изменение архитектуры системы
c. Хищение данных, подкуп системных администраторов, нарушение регламента работы

14. Виды информационной безопасности:

Выберите один ответ.

a. Персональная, корпоративная, государственная
b. Клиентская, серверная, сетевая
c. Локальная, глобальная, смешанная

15. Цели информационной безопасности – своевременное обнаружение, предупреждение:

Выберите один ответ.

a.несанкционированного доступа, воздействия в сети
b. инсайдерства в организации
c.чрезвычайных ситуаций

16. Основные объекты информационной безопасности:

Выберите один ответ.

a. Компьютерные сети, базы данных
b. Информационные системы, психологическое состояние пользователей
c. Бизнес-ориентированные, коммерческие системы

Вариант 2

1. Основные угрозы доступности информации:

1) непреднамеренные ошибки пользователей
2) злонамеренное изменение данных
3) хакерская атака
4) отказ программного и аппаратного обеспечения
5) разрушение или повреждение помещений
6) перехват данных

2. Суть компрометации информации.

1) внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации
2) несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений
3) внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений

3. Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она, ...

1) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой - ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды
2) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации
3) способна противостоять только информационным угрозам, как внешним так и внутренним
4) способна противостоять только внешним информационным угрозам

4. Методы повышения достоверности входных данных.

1) Замена процесса ввода значения процессом выбора значения из предлагаемого множества
2) Отказ от использования данных
3) Проведение комплекса регламентных работ
4) Использование вместо ввода значения его считывание с машиночитаемого носителя
5) Введение избыточности в документ первоисточник
6) Многократный ввод данных и сличение введенных значений

5. Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ).
1) МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения
2) МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты
3) МЭ работают только на сетевом уровне, а СОВ – еще и на физическом

6. Сервисы безопасности:
1) идентификация и аутентификация
2) шифрование
3) инверсия паролей
4) контроль целостности
5) регулирование конфликтов
6) экранирование
7) обеспечение безопасного восстановления
8) кэширование записей

7. Под угрозой удаленного администрирования в компьютерной сети понимается угроза ...
1) несанкционированного управления удаленным компьютером
2) внедрения агрессивного программного кода в рамках активных объектов Web-страниц
3) перехвата или подмены данных на путях транспортировки
4) вмешательства в личную жизнь
5) поставки неприемлемого содержания

8. Причины возникновения ошибки в данных.
1) Погрешность измерений
2) Ошибка при записи результатов измерений в промежуточный документ
3) Неверная интерпретация данных
4) Ошибки при переносе данных с промежуточного документа в компьютер
5) Использование недопустимых методов анализа данных
6) Неустранимые причины природного характера
7) Преднамеренное искажение данных
8) Ошибки при идентификации объекта или субъекта хозяйственной деятельности

9. К формам защиты информации не относится...
1) аналитическая
2) правовая
3) организационно-техническая
4) страховая

10. Наиболее эффективное средство для защиты от сетевых атак.
1) использование сетевых экранов или "firewall"

2) использование антивирусных программ
3) посещение только "надёжных" Интернет-узлов
4) использование только сертифицированных программ-браузеров при доступе к сети Интернет.

11. Информация, составляющая государственную тайну не может иметь гриф...
1) "для служебного пользования"
2) "секретно"
3) "совершенно секретно"
4) "особой важности"

12. Разделы современной криптографии:
1) Симметричные криптосистемы
2) Криптосистемы с открытым ключом
3) Криптосистемы с дублированием защиты
4) Системы электронной подписи
5) Управление паролями
6) Управление передачей данных
7) Управление ключами

13. Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности.
1) рекомендации X.800
2) Оранжевая книга
3) Закону "Об информации, информационных технологиях и о защите информации"

14. Утечка информации – это ...
1) несанкционированный процесс переноса информации от источника к злоумышленнику
2) процесс раскрытия секретной информации
3) процесс уничтожения информации
4) непреднамеренная утрата носителя информации

15. Основные угрозы конфиденциальности информации
1) маскарад
2) карнавал
3) переадресовка
4) перехват данных
5) блокирование
6) злоупотребления полномочиями

16. Элементы знака охраны авторского права:
1) буквы С в окружности или круглых скобках
2) буквы Р в окружности или круглых скобках
3) наименования (имени) правообладателя
4) наименование охраняемого объекта
5) года первого выпуска программы

17. Защита информации обеспечивается применением антивирусных средств
1) да
2) нет
3) не всегда

18. Средства защиты объектов файловой системы основаны на…
1) определении прав пользователя на операции с файлами и каталогами
2) задании атрибутов файлов и каталогов, независящих от прав пользователей

19. Вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование - ... угроза
1) активная
2) пассивная

20. Преднамеренная угроза безопасности информации
1) кража
2) наводнение
3) повреждение кабеля, по которому идет передача, в связи с погодными условиями
4) ошибка разработчика

21. Концепция системы защиты от информационного оружия не должна включать…
1) средства нанесения контратаки с помощью информационного оружия
2) механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры
3) признаки, сигнализирующие о возможном нападении
4) процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей

22. В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на ...
1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации
2) реализацию права на доступ к информации
3) соблюдение норм международного права в сфере информационной безопасности
4) выявление нарушителей и привлечение их к ответственности
5) соблюдение конфиденциальности информации ограниченного доступа
6) разработку методов и усовершенствование средств информационной безопасности

23.Компьютерные вирусы - это:
1) вредоносные программы, которые возникают в связи со сбоями в аппаратных средствах компьютера
2) программы, которые пишутся хакерами специально для нанесения ущерба пользователям ПК
3) программы, являющиеся следствием ошибок в операционной системе
4) вирусы, сходные по природе с биологическими вирусами

24. Что не относится к объектам информационной безопасности РФ?
1) природные и энергетические ресурсы
2) информационные системы различного класса и назначения, информационные технологии
3) система формирования общественного сознания
4) права граждан, юридических лиц и государства на получение, распространение, использование и защиту информации и интеллектуальной собственности.

25. Какие действия в Уголовном кодексе РФ классифицируются как преступления в компьютерной информационной сфере?
1) неправомерный доступ к компьютерной информации
2) создание, использование и распространение вредоносных программ для ЭВМ
3) умышленное нарушение правил эксплуатации ЭВМ и их сетей
4)все перечисленное выше

Зачетно-экзаменационные материалы для промежуточной аттестации (зачет)

1. Цели государства в области обеспечения информационной безопасности.
2. Основные нормативные акты РФ, связанные с правовой защитой информации.
3. Виды компьютерных преступлений.
4. Способы и механизмы совершения информационных компьютерных преступлений.
5. Основные параметры и черты информационной компьютерной преступности в России.
6. Компьютерный вирус. Основные виды компьютерных вирусов.
7. Методы защиты от компьютерных вирусов.
8. Типы антивирусных программ.
9. Защиты от несанкционированного доступа. Идентификация и аутентификация пользователя.
10. Основные угрозы компьютерной безопасности при работе в сети Интернет.
11. Виды защищаемой информации.
12. Государственная тайна как особый вид защищаемой информации.
13. Конфиденциальная информация.
14. Система защиты государственной тайны.
15. Правовой режим защиты государственной тайны.
16. Защита интеллектуальной собственности средствами патентного и авторского права.
17. Международное законодательство в области защиты информации.
18. Программно-аппаратные средства обеспечения информационной безопасности в информационных сетях.
19. Симметричные шифры.
20. Ассиметричные шифры.
21. Криптографические протоколы.
22. Криптографические хеш-функции.
23. Электронная подпись.
24. Организационное обеспечение информационной безопасности.
25. Служба безопасности организации.
26. Методы защиты информации от утечки в технических каналах.
27. Инженерная защита и охрана объектов.

Критерии оценивания результатов обучения

Оценка	Критерии оценивания по зачету
зачтено	Высокий уровень (студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы).
	Средний уровень (студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные

	задания не оценены максимальным числом баллов, в основном сформировал практические навыки).
	Пороговый уровень (студент, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы).
не зачтено	Минимальный уровень (студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы).

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 экзамене;

– 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 : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490277

2. Внуков, А. А. Защита информации в банковских системах : учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490278

3. *Зенков, А. В.* Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный //

Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497002

4. *Суворова, Г. М.* Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496741

5. *Щеглов, А. Ю.* Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490019

3. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498844

4. *Корабельников, С. М.* Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2022. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496492

5. *Казарин, О. В.* Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2022. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493262

6. *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, 2022. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489745

7. *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, 2022. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490421

5.2. Периодическая литература

1. Базы данных компании «Ист Вью» http://dlib.eastview.com
2. Электронная библиотека GREBENNIKON.RU https://grebennikon.ru/

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

Электронно-библиотечные системы (ЭБС):

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

Профессиональные базы данных:

1. **Scopus** http://www.scopus.com/
2. **ScienceDirect** https://www.sciencedirect.com/
3. **Журналы издательства Wiley** https://onlinelibrary.wiley.com/

4. **Научная электронная библиотека (НЭБ)** http://www.elibrary.ru/
5. **Полнотекстовые архивы ведущих западных научных журналов на Российской платформе научных журналов НЭИКОН** http://archive.neicon.ru
6. **Национальная электронная библиотека** (доступ к Электронной библиотеке диссертаций Российской государственной библиотеки (РГБ) https://rusneb.ru/
7. **Президентская библиотека им. Б.Н. Ельцина** https://www.prlib.ru/
8. **База данных CSD Кембриджского центра кристаллографических данных (CCDC)** https://www.ccdc.cam.ac.uk/structures/
9. **Springer Journals:** https://link.springer.com/
10. **Springer Journals Archive:** https://link.springer.com/
11. **Nature Journals:** https://www.nature.com/
12. **Springer Nature Protocols and Methods**: https://experiments.springernature.com/sources/springer-protocols
13. **Springer Materials:** http://materials.springer.com/
14. **Nano Database:** https://nano.nature.com/
15. **Springer eBooks (i.e. 2020 eBook collections):** https://link.springer.com/
16. **"Лекториум ТВ"** http://www.lektorium.tv/
17. **Университетская информационная система РОССИЯ** http://uisrussia.msu.ru

Информационные справочные системы:

1. Консультант Плюс – справочная правовая система (доступ по локальной сети с компьютеров библиотеки)

Ресурсы свободного доступа:

1. **КиберЛенинка** http://cyberleninka.ru/;
2. **Американская патентная база данных** http://www.uspto.gov/patft/
3. **Министерство науки и высшего образования Российской Федерации** https://www.minobrnauki.gov.ru/;
4. **Федеральный портал "Российское образование"** http://www.edu.ru/;
5. **Информационная система "Единое окно доступа к образовательным ресурсам"** http://window.edu.ru/;
6. **Единая коллекция цифровых образовательных ресурсов** http://school-collection.edu.ru/ .
7. **Проект Государственного института русского языка имени А.С. Пушкина "Образование на русском"** https://pushkininstitute.ru/;
8. **Справочно-информационный портал "Русский язык"** http://gramota.ru/;
9. **Служба тематических толковых словарей** http://www.glossary.ru/;
10. **Словари и энциклопедии** http://dic.academic.ru/;
11. **Образовательный портал "Учеба"** http://www.ucheba.com/;
12. **Законопроект "Об образовании в Российской Федерации". Вопросы и ответы** http://xn--273--84d1f.xn--p1ai/voprosy_i_otvety

Собственные электронные образовательные и информационные ресурсы КубГУ:

1. **Электронный каталог Научной библиотеки КубГУ** http://megapro.kubsu.ru/MegaPro/Web
2. **Электронная библиотека трудов ученых КубГУ** http://megapro.kubsu.ru/MegaPro/UserEntry?Action=ToDb&idb=6
3. **Среда модульного динамического обучения** http://moodle.kubsu.ru
4. **База учебных планов, учебно-методических комплексов, публикаций и конференций** http://infoneeds.kubsu.ru/

5. **Библиотека информационных ресурсов кафедры информационных образовательных технологий** http://mschool.kubsu.ru;
6. **Электронный архив документов КубГУ** http://docspace.kubsu.ru/
7. **Электронные образовательные ресурсы кафедры информационных систем и технологий в образовании КубГУ и научно-методического журнала "ШКОЛЬНЫЕ ГОДЫ"** http://icdau.kubsu.ru/

6. Методические указания для обучающихся по освоению дисциплины (модуля)

Лекционные занятия проводятся по основным разделам дисциплины «Криптография и информационная безопасность». Они дополняются лабораторными работами, в ходе которых студенты выполняют задания по всем предлагаемым темам.

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	Занятия лекционного и лабораторного типа	Методические указания для подготовки к занятиям лекционного и семинарского типа. Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ». Протокол № 1 от 30 августа 2018 года. Режим доступа: https://www.kubsu.ru/ru/econ/metodicheskie-ukazaniya
2	Выполнение самостоятельной работы обучающихся	Методические указания по выполнению самостоятельной работы обучающихся. Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ». Протокол № 1 от 30 августа 2018 года. Режим доступа: https://www.kubsu.ru/ru/econ/metodicheskie-ukazaniya
3	Подготовка эссе, рефератов	Методические указания для подготовки эссе, рефератов, курсовых работ. Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ». Протокол № 1 от 30 августа 2018 года. Режим доступа:https://www.kubsu.ru/ru/econ/metodicheskie-ukazaniya
4	Интерактивные методы обучения	Методические указания по интерактивным методам обучения. Утверждены на заседании Совета экономического факультета ФГБОУ ВО «КубГУ». Протокол № 1 от 30 августа 2018 года. Режим доступа: https://www.kubsu.ru/ru/econ/metodicheskie-ukazaniya

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 (модулю)

По всем видам учебной деятельности в рамках дисциплины используются аудитории, кабинеты и лаборатории, оснащенные необходимым специализированным и лабораторным оборудованием.

Наименование специальных помещений	Оснащенность специальных помещений	Перечень лицензионного программного обеспечения
Учебные аудитории для проведения занятий лекционного типа	Мебель: учебная мебель Технические средства обучения: экран, проектор, ноутбук	Microsoft Windows 8, 10, Microsoft Office Professional Plus
Учебные аудитории для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Мебель: учебная мебель Технические средства обучения: экран, проектор, ноутбук	Microsoft Windows 8, 10, Microsoft Office Professional Plus

Учебные аудитории для проведения лабораторных работ:		
Лаборатория информационных и управляющих систем 201Н Лаборатория экономической информатики 202Н	Мебель: учебная мебель Технические средства обучения: экран, проектор, компьютеры, ноутбуки Оборудование: ПК, Терминальные станции, Усилитель автономный беспроводной	Microsoft Windows 8, 10, Microsoft Office Professional Plus
Лаборатория управления в технических системах 207Н	Типовой комплект учебного оборудования "Теория автоматического управления", Презентации и плакаты Усилитель автономный беспроводной с микрофоном	Microsoft Windows 8, 10, Microsoft Office Professional Plus
Лаборатория организационно-технологического обеспечения торговой и маркетинговой деятельности 201А	Панель интерактивная, Конференц-система, Микшер-усилитель, Подавитель акустической обратной связи, Настенный громкоговоритель, Радиосистема, Микрофон на гибком держателе, Моноблок HP, Документ-камера, Беспроводная точка доступа, Система видеоотображения, ЖК панель Сплитер, Мультимедийная трибуна лектор, Система видеоконференцсвязи, Плакаты	Microsoft Windows 8, 10, Microsoft Office Professional Plus
Лаборатория экономики и управления 212Н	Презентации и плакаты, Многофункциональный профессиональный видео детектор банкнот и ценных бумаг, Счетчики банкнот, Инфракрасный детектор банкнот и ценных бумаг, Универсальный детектор банкнот и ценных бумаг, Детектор подлинности банкнот, Ящик денежный, Планшетный импринтер, Усилитель автономный беспроводной	Microsoft Windows 8, 10, Microsoft Office Professional Plus
Лаборатория безопасности жизнедеятельности 105А	Лабораторные стенды, Типовой комплект учебного оборудования, Стенды-тренажеры, Стенд-планшет, Тренажерный комплекс по применению первичных средств пожаротушения, Комплекс – тренажер по оказанию первой доврачебной помощи, Робот-тренажер, Комплект	Microsoft Windows 8, 10, Microsoft Office Professional Plus

	плакатов, Комплект демонстрационных пособий, Комплект аудиовизуальных пособий	

Для самостоятельной работы обучающихся предусмотрены помещения, укомплектованные специализированной мебелью, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

Наименование помещений для самостоятельной работы обучающихся	Оснащенность помещений для самостоятельной работы обучающихся	Перечень лицензионного программного обеспечения
Помещение для самостоятельной работы обучающихся (читальный зал Научной библиотеки)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	Microsoft Windows 8, 10, Microsoft Office Professional Plus
Помещение для самостоятельной работы обучающихся (ауд.213 А, 218 А)	Мебель: учебная мебель Комплект специализированной мебели: компьютерные столы Оборудование: компьютерная техника с подключением к информационно-коммуникационной сети «Интернет» и доступом в электронную информационно-образовательную среду образовательной организации, веб-камеры, коммуникационное оборудование, обеспечивающее доступ к сети интернет (проводное соединение и беспроводное соединение по технологии Wi-Fi)	Microsoft Windows 8, 10, Microsoft Office Professional Plus