МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет экономический

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) Б1.В.ДЭ.1.1«Кибербезопасность в финансовой сфере»

Направление подготовки/специальность *38.04.08 Финансы и кредит*

Направленность (профиль) / специализация *Финансы в цифровой экономике*

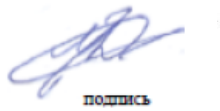
Форма обучения *очная*

Квалификация магистратура

Краснодар 2024

Рабочая программа дисциплины «Информационно-аналитические системы и технологии в финансовой сфере» составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 38.04.08 Финансы и кредит

Программу составил (и):



Мельник Д.В., преподаватель кафедры анализа данных и искусственного интеллекта.

Рабочая программа дисциплины «Информационно-аналитические системы и технологии в финансовой сфере» утверждена на заседании кафедры анализа данных и искусственного интеллекта протокол № 9 от 20 мая 2024 г.

Заведующая КАДИИ Коваленко А.В.

Утверждена на заседании учебно-методической комиссии факультета компьютерных технологий и прикладной математики протокол № 3 от 21 мая 2024 г.

Председатель УМК факультета
Л.Н. Дробышевская
доктор экон. наук, профессор

Рецензенты:

Гончаров С.В., директор ООО «ПВС»
Оломская Е.В., канд. экон. наук, доцент кафедры бухгалтерского учета, аудита и автоматизированной обработки данных ФГБОУ ВО «Кубанский государственный университет»

Цели и задачи изучения дисциплины.

1.1 Цель освоения дисциплины.

Дисциплиа посвящен изучению современных концепций информационной безопасности и их применения в обеспечении защиты информации и безопасного использования программных средств в вычислительных системах. Цель дисциплины – научить студента методам информационной безопасности и их использовании в области защиты информации.

Воспитательной целью дисциплины является формирование у студентов научного, творческого подхода к освоению технологий, методов и средств производства и защиты программного обеспечения. Дать студентам математические основы защиты информации.

Отбор материала основывается на необходимости ознакомить студентов со следующей современной научной информацией: методы защиты информации; области применения защиты информации; о технологиях анализа шифров.

Содержательное наполнение дисциплины обусловлено общими задачами в подготовке магистра.

Научной основой для построения программы данной дисциплины является теоретико-прагматический подход в обучении.

Студент должен осуществлять профессиональную деятельность и уметь решать задачи, соответствующие программе дисциплины.

Студент после освоения дисциплины приобретает теоретические знания и практические навыки в области применения задач информационной безопасности; методов защиты информации; области применения различных методов информационной безопасности; этапы, методы и инструментальные средства информационной безопасности; принципах построения и функционирования систем информационной безопасности; классификации шифров; основах организации идентификации и цифровой подписи; принципах построения и применения паролей; умеет проводить анализ и определять оптимальный метод защиты информации; формировать требования к предметноориентированной системе информационной безопасности и определять возможные пути их выполнения; формулировать и решать задачи организации процесса цифровой подписи; формулировать и решать задачи организации процесса идентификации; реализовать на языке программирования заданный метод защиты информации; решать задачи анализа шифра.

В качестве основной формы итогового контроля по рассматриваемой дисциплине предусмотрен экзамен.

1.2 Задачи дисциплины.

Задачей дисциплины является изложение теории информационной безопасности и практики применения алгоритмов криптозащиты. Основные задачи дисциплины на основе системного подхода:

- Описать проблемную область информационной безопасности.
- Дать описание практического применения теории конечных полей в теории защиты информации.
- Расширить понятия о генерации псевдослучайных последовательностях.

- Расширить понятия о способах защиты информации.
- Расширить понятия о методах построения современных программных систем.
- Дать навыки практической работы с методами защиты информации.
- Дать навыки практической работы по решению задач идентификации.
- Дать навыки практической работы по решению задач цифровой подписи.

Содержательное наполнение дисциплины обусловлено общими задачами в подготовке магистра.

Научной основой для построения программы данной дисциплины является теоретико-прагматический подход в обучении.

1.3 Место дисциплины в структуре образовательной программы.

Дисциплина «Современные технологии передачи и защиты информации» входит в базовую часть Блока 1 «Дисциплины (модули)» дисциплин, формирующих знания и навыки в области разработки современного программного обеспечения. Дисциплина опирается на знания в области дискретной математики, математической логики, программирования, базы данных. Дисциплина расширяет знания студентов в области создания программных систем, защиты данных и знаний.

Дисциплина тесно связана с дисциплинами «Математическое моделирование информационных систем и процессов», «Высокопроизводительные технологии программирования».

К результатам обучения относятся: фундаментальная подготовка по основам профессиональных знаний; способность понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе; соблюдение основных требований информационной безопасности, в том числе защиты государственной тайны владение основными методами, способами и средствами получения, хранения, переработки информации, имеет навыки работы с компьютером как средством управления информацией способность к анализу и синтезу; способность определения общих форм, закономерностей, инструментальных средств данной дисциплины; умение

понять поставленную задачу

умение грамотно пользоваться языком предметной области;

умение извлекать полезную научно-техническую информацию из электронных библиотек, реферативных журналов, сети Интернет знание математических

основ информатики как науки

знание проблемы современной информатики, ее категории и связи с другими научными дисциплинами; знание содержания, основных этапов и тенденции развития

программирования,

математического обеспечения и информационных технологий.

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

Студент должен осуществлять профессиональную деятельность и уметь решать задачи, соответствующие программе дисциплины.

Знать	1) области применения задач информационной безопасности; 2) стандарты шифрования; 3) методы защиты информации; 4) области применения различных методов информационной безопасности;
	5) этапы, методы и инструментальные средства информационной безопасности. 6) принципы построения и функционирования систем информационной безопасности; 7) способностью разрабатывать и анализировать концептуальные и теоретические модели 8) классификацию шифров; 9) основы организации идентификации и цифровой подписи; 10) принципы построения и применения паролей; 11) правовые и этические последствия при получении доступа к информации не санкционированным лица
Уметь	12) проводить анализ и определять оптимальный метод защиты информации; 13) формировать требования к предметно-ориентированной системе информационной безопасности и определять возможные пути их выполнения; 14) анализировать модели шифрования при организации защиты данных 15) формулировать и решать задачи организации процесса цифровой подписи; 16) формулировать и решать задачи организации процесса идентификации; 17) реализовать на языке программирования заданный метод защиты информации; 18) использовать математический аппарат определяющий шифр; 19) решать задачи анализа шифра; 20) оценить последствия при компрометации ключа или шифра
Владеть	21) методологиями и парадигмами построение систем информационной безопасности; 22) методами проектирования систем защиты информации; 23) методами построения алгоритмов анализа; 24) методами построения систем идентификации; 25) методами определения требований и состава средств, мероприятий по системе информационной безопасности систем; 26) навыками оценки правовых и этических компрометации данных 27) методами определения и создания шифра

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
1.	ОПК-5	способностью использовать углубленные знания правовых и этических норм при оценке последствий своей профессиональной деятельности, при разработке и осуществлении социально значимых проектов	1, 2, 3, 5, 6, 9, 10	12, 13, 19, 20	25, 26
2.	ОК-2	готовностью действовать в нестандартных ситуациях, нести социальную и этическую ответственность за принятые решения	2, 4, 5, 6, 10	12, 13, 20	22, 25,26
3.	ПК-2	способностью использовать углубленные теоретические и	2, 3, 5, 7, 9	14, 15, 16	21, 22, 23, 24
№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
		практические знания в области информационных технологий и прикладной математики, фундаментальных концепций и системных методологий, международных и профессиональных стандартов в области информационных технологий			
4.	ПК-5	способностью управлять проектами, планировать научноисследовательскую деятельность, анализировать риски, управлять командой проекта	1, 2, 5, 7, 8, 10	12, 17, 18, 19, 20	23, 24, 25, 27

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 5зач.ед. (180 часов), их распределение по видам работ представлено в таблице:

Вид учебной работы	Всего часов	Семестры(часы)			
		1	___		

Контактная работа, в том числе:						
Аудиторные занятия (всего):		72				
Занятия лекционного типа		24		-	-	-
Лабораторные занятия		47,8		-	-	-
Иная контактная работа:						
Промежуточная аттестация (ИКР)		0,3				
Самостоятельная работа, в том числе:						
Проработка учебного (теоретического) материала		20,8		-	-	-
Выполнение индивидуальных заданий		27		-	-	-
Подготовка к текущему контролю		-		-	-	-
Контроль:						
Подготовка к экзамену		-				
Общая трудоемкость	**час.**	**72**		**-**	**-**	**-**
	в том числе контактная работа	**24,2**				
	зач. ед	**2**				

Процедура промежуточной аттестации проходит в форме экзамена.

2.2 Структура дисциплины: Распределение видов учебной работы и их трудоемкости по разделам дисциплины. Разделы дисциплины, изучаемые в 1 семестре (очная форма). Вид промежуточной аттестации: экзамен.

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа		Внеаудиторная работа	
			Л	ЛР	СР	контроль
1.	Базовые понятия и история развития информационной безопасности.	4	2	2	1,8	1,8
2	Конечные поля. Многочлены над конечным полем. Последовательности над конечным полем.	15	3	3	2	2
3	Шифры замены. Шифры перестановки. Шифры гаммирования.	21	3	3	2	2
3	Блочные системы шифрования.	15	3	3	2	2
3	Поточные системы шифрования.	13	3	3	2	2
3	Идентификация. Цифровые подписи.	17	2	2	2,2	2,2
2	Промежуточная аттестация (ИКР)	1			2	2
	Итого по дисциплине:	72	24	47	47,8	14
16						

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

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа.

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1.	Базовые понятия и история развития информационной безопасности.	Защита информации. Угрозы информационной безопасности. Угрозы информационной безопасности.	собеседование
2.	Конечные поля. Многочлены над конечным полем. Последовательности над конечным полем.	Конечные поля. Характеристика поля. Мультипликативная группа конечного поля. Неприводимые многочлены. Порядок многочлена над конечным полем. Последовательности над конечным полем. Псевдослучайные последовательности и их применение. Линейные рекуррентные последовательности над конечным полем. Линейные рекуррентные последовательности как псевдослучайные последовательности.	собеседование, индивидуальное задание
3.	Шифры замены. Шифры перестановки. Шифры гаммирования.	Математическая модель шифра замены. Классификация шифров замены. Поточные шифры простой замены. Криптоанализ поточного шифра простой замены. Блочные шифры простой замены. Многоалфавитные шифры замены. Дисковые многоалфавитные шифры замены. Шифры перестановки. Маршрутные перестановки. Элементы криптоанализа шифров перестановки. Табличное гаммирование. О возможности восстановления вероятностей знаков гаммы.	собеседование, индивидуальное задание
4.	Блочные системы шифрования.	Блочные системы шифрования. Принципы построения блочных шифров. Американский стандарт шифрования данных DES. Стандарт шифрования данных ГОСТ 28147-89. Методы	собеседование, индивидуальное задание
		анализа алгоритмов блочного шифрования	
5.	Поточные системы шифрования.	Поточные системы шифрования. Шифрсистема A5. ШифрсистемаГиффорда. Линейные регистры сдвига. Алгоритм Берлекемпа—Месси. Методы анализа поточных шифров.	собеседование, индивидуальное задание
6.	Идентификация. Цифровые подписи.	Идентификация. Фиксированные пароли. Парольные фразы. Атаки на фиксированные пароли. Одноразовые пароли. Протоколы с нулевым разглашением. Атаки на протоколы идентификации. Цифровые подписи. Цифровая подпись Фиата-Шамира. Цифровая подпись ЭльГамаля. Одноразовые цифровые подписи.	собеседование, индивидуальное задание

2.3.2 Занятия семинарского типа.

Не предусмотрены

2.3.3 Лабораторные занятия.

№	Наименование лабораторных работ	Форма текущего контроля
1.	Основные шифры.	индивидуальное задание
2.	Стойкость шифров.	индивидуальное задание
3.	Конечные поля. Характеристика поля. Мультипликативная группа конечного поля.	индивидуальное задание
4.	Неприводимые многочлены. Порядок многочлена над конечным полем. Последовательности над конечным полем.	индивидуальное задание
5.	Последовательности над конечным полем. Псевдослучайные последовательности и их применение. Линейные рекуррентные последовательности над конечным полем. Линейные рекуррентные последовательности как псевдослучайные последовательности.	индивидуальное задание
6.	Математическая модель шифра замены. Поточные шифры простой замены. Блочные шифры простой замены.	индивидуальное задание
7.	Многоалфавитные шифры замены. Шифры перестановки. Маршрутные перестановки.	индивидуальное задание
8.	Табличное гаммирование.	индивидуальное задание
9.	Принципы построения блочных шифров.	индивидуальное задание
10.	Американский стандарт шифрования данных DES и его модификации.	индивидуальное задание
11.	Стандарт шифрования данных ГОСТ 28147-89. Методы анализа алгоритмов блочного шифрования	индивидуальное задание
12.	Поточные системы шифрования.	индивидуальное задание
13.	Линейные регистры сдвига.	индивидуальное задание
14.	Методы анализа поточных шифров.	индивидуальное задание
15.	Идентификация. Фиксированные пароли. Парольные фразы.	индивидуальное задание
16.	Цифровые подписи. Одноразовые цифровые подписи.	индивидуальное задание

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	Базовые понятия и история развития информационной безопасности.	Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, И. П. Слинькова, В. В. Гафнер, П. А. Кисляков ; М-во образования и науки Рос. Федерации, ФГБОУ ВПО "Новосибирский гос. пед. ун-т", ФГБОУ ВПО "Моск. пед. гос. ун-т". - Москва ; Новосибирск : [АРТА], 2012 Стандарты оформления исходного кода программ и современные интегрированные среды разработки программного обеспечения: учеб.-метод.пособие. Ю.В. Кольцов [и др.] – Краснодар: Кубанский гос.ун-т, 2017 Financial Cybersecurity Risk Management: Leadership Perspectives and Guidance for Systems and Institutions». 12 Авторы: Paul Rohmeyer и Jennifer L. Bayuk. Книга вышла в 2018 Управление рисками финансовой кибербезопасности: перспективы лидерства и рекомендации для систем и учреждений. Авторы: Пол Ромайер и Дженнифер Л. Баюк. 2018.
2	Конечные поля. Многочлены над конечным полем. Последовательности над конечным полем.	Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, И. П. Слинькова, В. В. Гафнер, П. А. Кисляков ; М-во образования и науки Рос. Федерации, ФГБОУ ВПО "Новосибирский гос. пед. ун-т", ФГБОУ ВПО "Моск. пед. гос. ун-т". - Москва ; Новосибирск : [АРТА], 2012 Стандарты оформления исходного кода программ и современные интегрированные среды разработки программного обеспечения: учеб.-метод.пособие. Ю.В. Кольцов [и др.] – Краснодар: Кубанский гос.ун-т, 2017 Financial Cybersecurity Risk Management: Leadership Perspectives and Guidance for Systems and Institutions». 12 Авторы: Paul Rohmeyer и Jennifer L. Bayuk. Книга вышла в 2018 Управление рисками финансовой кибербезопасности: перспективы лидерства и рекомендации для систем и учреждений. Авторы: Пол Ромайер и Дженнифер Л. Баюк. 2018.
3	Шифры замены. Шифры перестановки. Шифры гаммирования.	Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, И. П. Слинькова, В. В. Гафнер, П. А. Кисляков ; М-во образования и науки Рос. Федерации, ФГБОУ ВПО "Новосибирский гос. пед. ун-т", ФГБОУ ВПО "Моск. пед. гос. ун-т". - Москва ; Новосибирск : [АРТА], 2012 Стандарты оформления исходного кода программ и современные интегрированные среды разработки программного обеспечения: учеб.-метод.пособие. Ю.В. Кольцов [и др.] – Краснодар: Кубанский гос.ун-т, 2017 Financial Cybersecurity Risk Management: Leadership Perspectives and Guidance for Systems and Institutions». 12 Авторы: Paul Rohmeyer и Jennifer L. Bayuk. Книга вышла в 2018 Управление рисками финансовой кибербезопасности: перспективы лидерства и рекомендации для систем и учреждений. Авторы: Пол Ромайер и Дженнифер Л. Баюк. 2018.
4	Блочные системы шифрования.	Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, И. П. Слинькова, В. В. Гафнер, П. А. Кисляков ; М-во образования и науки Рос. Федерации, ФГБОУ ВПО "Новосибирский гос. пед. ун-т", ФГБОУ ВПО "Моск. пед. гос. ун-т". - Москва ; Новосибирск : [АРТА], 2012 Стандарты оформления исходного кода программ и современные интегрированные среды разработки программного обеспечения: учеб.-метод.пособие. Ю.В. Кольцов [и др.] – Краснодар: Кубанский гос.ун-т, 2017 Financial Cybersecurity Risk Management: Leadership Perspectives and Guidance for Systems and Institutions». 12 Авторы: Paul Rohmeyer и Jennifer L. Bayuk. Книга вышла в 2018 Управление рисками финансовой кибербезопасности: перспективы лидерства и рекомендации для систем и учреждений. Авторы: Пол Ромайер и Дженнифер Л. Баюк. 2018.

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
5	Поточные системы шифрования.	Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, И. П. Слинькова, В. В. Гафнер, П. А. Кисляков ; М-во образования и науки Рос. Федерации, ФГБОУ ВПО "Новосибирский гос. пед. ун-т", ФГБОУ ВПО "Моск. пед. гос. ун-т". - Москва ; Новосибирск : [АРТА], 2012 Стандарты оформления исходного кода программ и современные интегрированные среды разработки программного обеспечения: учеб.-метод.пособие. Ю.В. Кольцов [и др.] – Краснодар: Кубанский гос.ун-т, 2017 Financial Cybersecurity Risk Management: Leadership Perspectives and Guidance for Systems and Institutions». 12 Авторы: Paul Rohmeyer и Jennifer L. Bayuk. Книга вышла в 2018 Управление рисками финансовой кибербезопасности: перспективы лидерства и рекомендации для систем и учреждений. Авторы: Пол Ромайер и Дженнифер Л. Баюк. 2018.
6	Идентификация. Цифровые подписи.	Информационная безопасность : учебное пособие для студентов вузов / С. В. Петров, И. П. Слинькова, В. В. Гафнер, П. А. Кисляков ; М-во образования и науки Рос. Федерации, ФГБОУ ВПО "Новосибирский гос. пед. ун-т", ФГБОУ ВПО "Моск. пед. гос. ун-т". - Москва ; Новосибирск : [АРТА], 2012 Стандарты оформления исходного кода программ и современные интегрированные среды разработки программного обеспечения: учеб.-метод.пособие. Ю.В. Кольцов [и др.] – Краснодар: Кубанский гос.ун-т, 2017 Financial Cybersecurity Risk Management: Leadership Perspectives and Guidance for Systems and Institutions». 12 Авторы: Paul Rohmeyer и Jennifer L. Bayuk. Книга вышла в 2018 Управление рисками финансовой кибербезопасности: перспективы лидерства и рекомендации для систем и учреждений. Авторы: Пол Ромайер и Дженнифер Л. Баюк. 2018.

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,

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.

3. Образовательные технологии.

В соответствии с требованиями ФГОС в программа дисциплины предусматривает использование в учебном процессе следующих образовательные технологии: чтение лекций с использованием мультимедийных технологий; метод малых групп, разбор практических задач и кейсов.

При обучении используются следующие образовательные технологии:

− Технология коммуникативного обучения – направлена на формирование коммуникативной компетентности студентов, которая является базовой, необходимой для адаптации к современным условиям межкультурной коммуникации.

− Технология разноуровневого (дифференцированного) обучения – предполагает осуществление познавательной деятельности студентов с учётом их индивидуальных способностей, возможностей и интересов, поощряя их реализовывать свой творческий потенциал. Создание и использование диагностических тестов является неотъемлемой частью данной технологии.

− Технология модульного обучения – предусматривает деление содержания дисциплины на достаточно автономные разделы (модули), интегрированные в общий курс.

− Информационно-коммуникационные технологии (ИКТ) - расширяют рамки образовательного процесса, повышая его практическую направленность, способствуют интенсификации самостоятельной работы учащихся и повышению познавательной активности. В рамках ИКТ выделяются 2 вида технологий:

− Технология использования компьютерных программ – позволяет эффективно дополнить процесс обучения языку на всех уровнях.

− Интернет-технологии – предоставляют широкие возможности для поиска информации, разработки научных проектов, ведения научных исследований.

− Технология индивидуализации обучения – помогает реализовывать личностноориентированный подход, учитывая индивидуальные особенности и потребности учащихся.

− Проектная технология – ориентирована на моделирование социального взаимодействия учащихся с целью решения задачи, которая определяется в рамках профессиональной подготовки, выделяя ту или иную предметную область.

− Технология обучения в сотрудничестве – реализует идею взаимного обучения, осуществляя как индивидуальную, так и коллективную ответственность за решение учебных задач.

− Игровая технология – позволяет развивать навыки рассмотрения ряда возможных способов решения проблем, активизируя мышление студентов и раскрывая личностный потенциал каждого учащегося.

− Технология развития критического мышления – способствует формированию разносторонней личности, способной критически относиться к информации, умению отбирать информацию для решения поставленной задачи.

Комплексное использование в учебном процессе всех вышеназванных технологий стимулируют личностную, интеллектуальную активность, развивают познавательные процессы, способствуют формированию компетенций, которыми должен обладать будущий специалист.

Основные виды интерактивных образовательных технологий включают в себя: − работа в малых группах (команде) - совместная деятельность студентов в группе под руководством лидера, направленная на решение общей задачи путём творческого сложения

результатов индивидуальной работы членов команды с делением полномочий и ответственности;

− проектная технология - индивидуальная или коллективная деятельность по отбору, распределению и систематизации материала по определенной теме, в результате которой составляется проект;

− анализ конкретных ситуаций - анализ реальных проблемных ситуаций, имевших место в соответствующей области профессиональной деятельности, и поиск вариантов лучших решений;

− развитие критического мышления – образовательная деятельность, направленная на развитие у студентов разумного, рефлексивного мышления, способного выдвинуть новые идеи и увидеть новые возможности.

Подход разбора конкретных задач и ситуаций широко используется как преподавателем, так и студентами во время лекций, лабораторных занятий и анализа результатов самостоятельной работы. Это обусловлено тем, что при исследовании и решении каждой конкретной задачи имеется, как правило, несколько методов, а это требует разбора и оценки целой совокупности конкретных ситуаций.

Темы, задания и вопросы для самостоятельной работы призваны сформировать навыки поиска информации, умения самостоятельно расширять и углублять знания, полученные в ходе лекционных и практических занятий.

Подход разбора конкретных ситуаций широко используется как преподавателем, так и студентами при проведении анализа результатов самостоятельной работы.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

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.

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации.

4.1Фонд оценочных средств для проведения текущего контроля.

Индивидуальные задачи (выполняются студентами самостоятельно и предоставляются в письменном виде).

1. Алгоритм DES. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
2. Алгоритм A5. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
3. Алгоритм Feal. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
4. Алгоритм Crypto1. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
5. Алгоритм IDEA. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма Dragon. Реализовать в виде программного приложения с оконным интерфейсом.
6. Алгоритм ГОСТ 94. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
7. Алгоритм Mickey. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма Safer64. Реализовать в виде программного приложения с оконным интерфейсом.
8. Алгоритм Mosqito. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма RC5-64. Реализовать в виде программного приложения с оконным интерфейсом.
9. Алгоритм Rabbit. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
10. Алгоритм Loki 91. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма RC4. Реализовать в виде программного приложения с оконным интерфейсом.
11. Алгоритм CAST256. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
12. Алгоритм SEAL. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.
13. Алгоритм AES. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

14. Алгоритм GMR. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

15. Алгоритм Wake. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

16. Алгоритм Trivium. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

17. Алгоритм Skipjack. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

18. Алгоритм Vest. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

19. Алгоритм Frog. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

20. Алгоритм VMPC. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

21. Алгоритм Serpent. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

22. Алгоритм Oryx. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

23. Алгоритм TEA. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

24. Алгоритм Salsa20. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

25. Алгоритм Mars. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

26. Алгоритм Mugi. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

27. Алгоритм Blowfish. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

28. Алгоритм Pike. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

29. Алгоритм ГОСТ 2012. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

30. Алгоритм DSA. Описать NP-сложные задачи, лежащие в основе алгоритма. Криптостойкость алгоритма. Реализовать в виде программного приложения с оконным интерфейсом.

4.2 Фонд оценочных средств для проведения промежуточной аттестации.

Вопросы для промежуточной аттестациипо итогам освоения дисциплины:

1. Группа. Подгруппа.
2. Группа постановок.
3. Кольцо. Идеалы. Классы вычетов.
4. Кольца полиномов.
5. Конечные поля.
6. Кольцо вычетов.
7. Алгоритмы умножения, обращения, вычисления НОД.
8. Извлечение корней в конечном поле.
9. Вычисление символа Якоби. Проверка на простоту.
10. Основные понятия и определения криптографической защиты информации.
11. Шифрование.
12. Аутентификация.
13. Система RSA. Детерминированные методы разложения.
14. Система RSA. Вероятностные методы разложения.
15. Дискретное логарифмирование в конечном поле. Задача Диффи-Хеллмана.
16. Шифрование с открытым ключом для группы вычислимого порядка.
17. Шифрование с открытым ключом для группы трудновычислимого порядка.
18. Цифровая подпись на группе трудновычислимого порядка.
19. Цифровая подпись на группе вычислимого порядка.
20. Схемы предъявления битов. Криптографические протоколы доказательства с нулевым разглашением.
21. Криптографические протоколы передачи информации со стиранием. Криптографический протокол разделения секрета.
22. Криптографические протоколы управления ключами. Временная метка.

23. Основные понятия классической криптографии. Шифры замены и перестановки. Блочные шифры.
24. Режимы шифрования.
25. Шифр DES.
26. Шифр FEAL.
27. Шифр IDEA.
28. Шифр ГОСТ 28147-89.
29. Шифр RC5.
30. Шифр Blowfish.
31. Шифр SAFER.
32. Шифр AES.
33. Шифр MD5.
34. Шифр ГОСТ Р 34.11-94.
35. Хэш-функция. Хэширование.

Критерий оценивания:

Оценка		
Удовлетворительно	**Хорошо**	**Отлично**
• если студент указал направление решения задачи и получил «удовлетворительно» по двум вопросам • если студент верно решил задачу; получил «хорошо» или «отлично» по ответу хотя бы на один вопрос	• если студент в целом верно решил задачу и получил «хорошо» по двум вопросам • если студент в целом верно решил задачу и получил «удовлетворительно» по одному вопросу и «отлично» хотя бы на один вопрос	• если студент верно решил задачу и получил «хорошо» хотя бы по одному вопросу и «отлично» по другому

Оценка «неудовлетворительно» выставляется при невозможности поставить оценку «Удовлетворительно», «Хорошо», «Отлично»

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 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 основной и дополнительной учебной литературы, необходимой для освоения дисциплины.

5.1 Основная литература:

1. Прохорова, О.В. Информационная безопасность и защита информации : учебник /

О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурностроительный университет». - Самара : Самарский государственный архитектурностроительный университет, 2014. - http://biblioclub.ru/index.php?page=book&id=438331.

2. Лапонина, О.Р. Криптографические основы безопасности / О.Р. Лапонина. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016.

3. Петренко, В.И. Теоретические основы защиты информации : учебное пособие / В.И. Петренко ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «СевероКавказский федеральный университет». - Ставрополь : СКФУ, 2015. – https://biblioclub.ru/index.php?page=book_red&id=458204&sr=1

4. Фороузан, Б.А. Математика криптографии и теория шифрования / Б.А. Фороузан. -

2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - https://biblioclub.ru/index.php?page=book_red&id=428998&sr=1

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах «Лань» и «Юрайт».

5.2 Дополнительная литература:

1. Басалова, Г.В. Основы криптографии : курс лекций / Г.В. Басалова ; Национальный

Открытый Университет "ИНТУИТ". - Москва : Интернет-Университет Информационных Технологий, 2011. - 253 с. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=233689 2. Сергеева, Ю.С.

Защита информации. Конспект лекций [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : А-Приор, 2011. – https://biblioclub.ru/index.php?page=book_red&id=72670&sr=1 3. Голиков, А.М.

Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А.М. Голиков ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Томский государственный университет систем управления и радиоэлектроники, 2015. – https://biblioclub.ru/index.php?page=book_red&id=480637&sr=1

4. Долозов, Н.Л. Программные средства защиты информации : конспект лекций / Н.Л. Долозов, Т.А. Гультяева ; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. - Новосибирск : НГТУ, 2015. – https://biblioclub.ru/index.php?page=book_red&id=438307&sr=1
5. Бабенко, Л.И. Параллельные алгоритмы для решения задач защиты информации / Л.И. Бабенко, Е.А. Ищукова, И.Д. Сидоров. - Москва : Издательство Горячая линияТелеком, 2014. - https://e.lanbook.com/reader/book/63228/#1.

5.3. Периодические издания:

1. Вычислительные методы и программирование
2. Математическое моделирование
3. Прикладная информатика
4. Программирование

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

1. Назначение и структура алгоритмов шифрования— URL:http://www.ixbt.com/soft/alg-encryption.shtml
2. Криптографические алгоритмы, применяемые для обеспечения информационной безопасности при взаимодействии в

ИНТЕРНЕТURL:http://www.bnti.ru/showart.asp?aid=797&lvl=04.03.07.

7. Методические указания для обучающихся по освоению дисциплины.

По дисциплине предусмотрено проведение практических занятий, на которых дается прикладной систематизированный материал. В ходе занятий разбираются алгоритмы и структуры представления графов, а также приводятся примеры разработки программных приложений. После практического занятия рекомендуется выполнить упражнения, приводимые в аудитории для самостоятельной работы.

При самостоятельной работе студентов необходимо изучить литературу, приведенную в перечнях выше, для осмысления вводимых понятий, анализа предложенных подходов и методов разработки программ. Разрабатывая решение новой задачи студент должен уметь выбрать эффективные и надежные структуры данных для представления информации, подобрать соответствующие алгоритмы для их обработки, учесть специфику языка программирования, на котором будет выполнена реализация. Студент должен уметь выполнять тестирование и отладку алгоритмов решения задач с целью обнаружения и устранения в них ошибок.

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.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине.

8.1 Перечень информационных технологий.

– Проверка домашних заданий и консультирование посредством электронной почты.
– Использование электронных презентаций при проведении практических занятий.

8.2 Перечень необходимого программного обеспечения.

– КомпиляторязыкаC++(«MicrosoftVisualStudio 12»).
– Программы для демонстрации и создания презентаций («MicrosoftPowerPoint»). – Программы, поддерживающие OLE сервера(«MicrosoftWord», «MicrosoftExcel»).

8.3 Перечень информационных справочных систем:

1. Справочно-правовая система «Консультант Плюс» (http://www.consultant.ru)

2. Электронная библиотечная система eLIBRARY.RU (http://www.elibrary.ru)/

9. Материально-техническая база, необходимая для осуществления образовательногопроцесса по дисциплине.

№	Вид работ	Материально-техническое обеспечение дисциплины и оснащенность
1.	Лекционные занятия	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения
2.	Лабораторные занятия	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, проектором, программным обеспечением MS Windows, MicrosoftVisualStudio 12, MicrosoftPowerPoint, MicrosoftWord, MicrosoftExcel
3.	Текущий контроль, промежуточная аттестация	Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, компьютерами, программным обеспечением MS Windows, MicrosoftVisualStudio 12, MicrosoftPowerPoint, MicrosoftWord, MicrosoftExcel
4.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет»,программой экранного увеличения и обеспеченный доступом в электронную информационнообразовательную среду университета.

MINISTRY OF SCIENCE AND HIGHER EDUCATION OF THE RUSSIAN FEDERATION

Federal State Budgetary Educational Institution
higher education
"KUBAN STATE UNIVERSITY"
Faculty of Economics

WORK PROGRAM OF DISCIPLINE (MODULE) B1.V.DE.1.1 “Cybersecurity in the financial sector”

Direction of training/specialty *38.04.08 Finance and credit*

Focus (profile) / specialization *Finance in the digital economy*

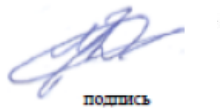
Form of study *full-time*

Qualification master's degree

Krasnodar 2024

The work program of the discipline “Information and analytical systems and technologies in the financial sector” is compiled in accordance with the federal state educational standard of higher education (FSES HE) in the field of study 04/38/08 Finance and credit

The program was compiled by:



Melnik D.V., teacher at the Department of Data Analysis and Artificial Intelligence.

The work program of the discipline “Information and analytical systems and technologies in the financial sector” was approved at a meeting of the Department of Data Analysis and Artificial Intelligence, protocol No. 9 of May 20, 2024.

Head of CADIA Kovalenko A.V.

Minutes No. 3 of May 21, 2024 were approved at a meeting of the educational and methodological commission of the Faculty of Computer Technologies and Applied Mathematics.

Chairman of the faculty's educational
complex L.N. Drobyshevskaya
Doctor of Economics sciences, professor

Reviewers:

Goncharov S.V., Director of PVS LLC

Olomskaya E.V., Ph.D. econ. Sciences, Associate Professor of the Department of Accounting, Audit and Automated Data Processing of the Federal State Budgetary Educational Institution of Higher Education "Kuban State University"

Goals and objectives of studying the discipline.

1.1 The purpose of mastering the discipline.

The discipline is devoted to the study of modern concepts of information security and their application in ensuring the protection of information and the safe use of software in computing systems. The purpose of the discipline is to teach the student information security methods and their use in the field of information security.

The educational goal of the discipline is to develop in students a scientific, creative approach to mastering technologies, methods and means of producing and protecting software. Give students the mathematical foundations of information security.

The selection of material is based on the need to familiarize students with the following modern scientific information: methods of information security; areas of application of information security; about cipher analysis technologies.

The content of the discipline is determined by the general objectives in the preparation of a master's degree.

The scientific basis for constructing the program of this discipline is the theoretical-pragmatic approach to teaching.

The student must carry out professional activities and be able to solve problems corresponding to the discipline program.

After mastering the discipline, the student acquires theoretical knowledge and practical skills in the application of information security tasks; information security methods; areas of application of various information security methods; stages, methods and tools of information security; principles of construction and operation of information security systems; cipher classifications; basics of organization of identification and digital signature; principles of constructing and using passwords; knows how to analyze and determine the optimal method of protecting information; formulate requirements for a subject-oriented information security system and determine possible ways to fulfill them; formulate and solve problems of organizing the digital signature process; formulate and solve problems of organizing the identification process; implement a given method of information security in a programming language; solve cipher analysis problems.

An exam is provided as the main form of final control in the discipline under consideration.

1.2 Objectives of the discipline.

The objective of the discipline is to present the theory of information security and the practice of applying cryptographic protection algorithms. The main objectives of the discipline based on a systematic approach:

- Describe the problem area of information security.
- Give a description of the practical application of the theory of finite fields in the theory information protection.
- Expand the concepts of generating pseudo-random sequences.

• Expand the concepts of information security methods.

• Expand the concepts of methods for constructing modern software systems.

• Provide skills for practical work with information security methods.

• Provide practical skills in solving identification problems.

• Provide practical skills in solving digital signature problems.

The content of the discipline is determined by the general objectives in the preparation of a master's degree.

The scientific basis for constructing the program of this discipline is the theoretical-pragmatic approach to teaching.

1.3 Place of discipline in the structure of the educational program.

The discipline “Modern technologies for transmitting and protecting information” is included in the basic part of Block 1 “Disciplines (modules)” of disciplines that form knowledge and skills in the field of modern software development. The discipline is based on knowledge in the field of discrete mathematics, mathematical logic, programming, and databases. The discipline expands students' knowledge in the field of creating software systems, data protection and knowledge.

The discipline is closely related to the disciplines “Mathematical modeling of information systems and processes”, “High-performance programming technologies”.

The learning outcomes include: fundamental training in the basics of professional knowledge; the ability to understand the essence and significance of information in the development of a modern information society, to recognize the dangers and threats that arise in this process; compliance with basic information security requirements, including the protection of state secrets; knowledge of the basic methods, methods and means of obtaining, storing, processing information; has skills in working with a computer as a means of information management; ability to analyze and synthesize; the ability to determine general forms, patterns, instrumental means of this discipline; skill

understand the task at hand

ability to competently use the language of the subject area;

ability to extract useful scientific and technical information from electronic libraries, abstract journals, the Internet knowledge of mathematical

fundamentals of computer science as a science

knowledge of the problem of modern computer science, its categories and connections with other scientific disciplines; knowledge of the content, main stages and development trends

programming,

software and information technology.

1.4 List of planned learning outcomes in the discipline, correlated with the planned results of mastering the educational program.

The student must carry out professional activities and be able to solve problems corresponding to the discipline program.

Know	1) areas of application of information security tasks; 2) encryption standards; 3) methods of information security; 4) areas of application of various information security methods;
	5) stages, methods And tools information security. 6) principles of construction and operation of information security systems; 7) ability to develop and analyze conceptual and theoretical models 8) classification of ciphers; 9) basics of organizing identification and digital signature; 10) principles of constructing and using passwords; 11) legal and ethical consequences of gaining access to information by an unauthorized person
Be able to	12) conduct analysis and determine the optimal method of protecting information; 13) formulate requirements for a subject-oriented information security system and determine possible ways to fulfill them; 14) analyze encryption models when organizing data protection 15) formulate and solve problems of organizing the digital signature process; 16) formulate and solve problems of organizing the identification process; 17) implement a given method of information security in a programming language; 18) use a mathematical apparatus that determines the code; 19) solve problems of cipher analysis; 20) assess the consequences if a key or cipher is compromised
Own	21) methodologies and paradigms for building information security systems; 22) methods for designing information security systems; 23) methods for constructing analysis algorithms; 24) methods for constructing identification systems; 25) methods for determining the requirements and composition of tools, measures for the information security system; 26) skills in assessing legal and ethical data compromises 27) methods for determining and creating a cipher

No. p.p.	Index competencies	The content of the competency (or its parts)	As a result of studying academic discipline students must		
			know	be able to	own
1.	OPK-5	ability use in-depth knowledge of legal and ethical standards when assessing consequences his professional activities, in the development and implementation of socially significant projects	1, 2, 3, 5, 6, 9, 10	12, 13, 19, 20	25, 26
2.	OK-2	readiness act V non-standard situations, carry social And ethical responsibility for accepted solutions	2, 4, 5, 6, 10	12, 13, 20	22, 25,26
3.	PC-2	ability use in-depth theoretical and	2, 3, 5, 7, 9	14, 15, 16	21, 22, 23, 24
No. p.p.	Index competencies	The content of the competency (or its parts)	As a result of studying academic discipline students must		
			know	be able to	own
		practical knowledge in the field of information technologies and applied mathematics, fundamental concepts and systemic methodologies international And professional standards in areas of information technologies			
4.	PK-5	ability manage projects, to plan research activities, analyze risks, manage the project team	1, 2, 5, 7, 8, 10	12, 17, 18, 19, 20	23, 24, 25, 27

2. Structure and content of the discipline.

2.1 Distribution of the labor intensity of the discipline by type of work.

The total labor intensity of the discipline is 5 credit units. (180 hours), their distribution by type of work is presented in the table:

Type of educational work	Total hours	Semesters(hours)			
		1	___		

Contact work, including:						
Classroom lessons (total):		72				
Lecture-type classes		24		-	-	-
Laboratory exercises		47.8		-	-	-
Other contact work:						
Interim certification (ICR)		0.3				
Independent work, including:						
Study of educational (theoretical) material		20.8		-	-	-
Completing individual tasks		27		-	-	-
Preparation for current control		-		-	-	-
Control:						
Exam preparation		-				
Total labor intensity	**hour.**	**72**		**-**	**-**	**-**
	including contact work	**24.2**				
	zach. units	**2**				

The intermediate certification procedure takes the form of an exam.

2.2 Structure of the discipline: Distribution of types of educational work and their labor intensity by sections of the discipline. Sections of the discipline studied in the 1st semester (full-time). Type of intermediate certification: exam.

No.	**Name of sections**	**Number of hours**				
		Total	**Classroom Job**		**Extracurricular Job**	
			L	**LR**	**SR**	**control**
1.	Basic concepts And story development of information security.	4	2	2	1.8	1.8
2	End fields. Polynomials over a finite field. Sequences over a finite field.	15	3	3	2	2
3	Replacement ciphers. Permutation ciphers. Gamma ciphers.	21	3	3	2	2
3	Block encryption systems.	15	3	3	2	2
3	Stream encryption systems.	13	3	3	2	2
3	Identification. Digital signatures.	17	2	2	2.2	2.2
2	Interim certification (ICR)	1			2	2
	Total for the discipline:	72	24	47	47.8	14
16						

Note: L – lectures, PZ – practical classes/seminars, LR – laboratory classes, SR – student's independent work

2.3 Contents of discipline sections:

2.3.1 Lecture-type classes.

No.	Name section	Section Contents	Form current control
1.	Basic concepts and history of development informational security.	Data protection. Information security threats. Threats informational security.	interview
2.	Final fields. Polynomials above final field. Sequences over the final field.	Final fields. Characteristic fields. Multiplicative group of a finite field. Irreducible polynomials. The order of a polynomial over a finite field. Sequences over finite field. Pseudorandom sequences and their application. Linear recurrent sequences over a finite field. Linear recurrent sequences like pseudorandom sequences.	interview, individual exercise
3.	Replacement ciphers. Ciphers permutations. Ciphers gamming.	Mathematical model cipher replacements. Classification of replacement ciphers. Simple substitution stream ciphers. Cryptanalysis of a simple substitution stream cipher. Simple substitution block ciphers. Polyalphabetic substitution ciphers. Disk polyalphabetic substitution ciphers. Ciphers permutations. Route permutations. Elements of cryptanalysis of permutation ciphers. Tabular gamming. On the possibility of restoring the probabilities of gamma signs.	interview, individual exercise
4.	Block systems encryption.	Block systems encryption. Principles building block ciphers. American data encryption standard DES. Data encryption standard GOST 28147-89. Methods	interview, individual exercise
		analysis of block encryption algorithms	
5.	Flow systems encryption.	Stream encryption systems. A5 encryption system. Gifford cipher system. Linear shift registers. Berlekamp-Massey algorithm. Methods for analyzing stream ciphers.	interview, individual exercise
6.	Identification. Digital signatures.	Identification. Fixed passwords. Passphrases. Attacks on fixed passwords. One-time passwords. Zero knowledge protocols. Attacks on identification protocols. Digital signatures. Digital signature of Fiat-Shamir. ElGamal's digital signature. One-time digital signatures.	interview, individual exercise

2.3.2 Seminar-type classes.

Not provided

2.3.3 Laboratory exercises.

No.	Name of laboratory work	Form current control
1.	Basic ciphers.	individual exercise
2.	Strength of ciphers.	individual exercise
3.	End fields. Field characteristics. Multiplicative group of a finite field.	individual exercise
4.	Irreducible polynomials. The order of a polynomial over a finite field. Sequences over a finite field.	individual exercise
5.	Sequences over a finite field. Pseudorandom sequences and their applications. Linear recurrent sequences over a finite field. Linear recurrent sequences as pseudorandom sequences.	individual exercise
6.	Mathematical model of the substitution cipher. Simple substitution stream ciphers. Simple substitution block ciphers.	individual exercise
7.	Polyalphabetic substitution ciphers. Permutation ciphers. Route changes.	individual exercise
8.	Tabular gamming.	individual exercise
9.	Principles of constructing block ciphers.	individual exercise
10.	American data encryption standard DES and its modifications.	individual exercise
eleven.	Data encryption standard GOST 28147-89. Methods for analyzing block encryption algorithms	individual exercise
12.	Stream encryption systems.	individual exercise
13.	Linear shift registers.	individual exercise
14.	Methods for analyzing stream ciphers.	individual exercise
15.	Identification. Fixed passwords. Passphrases.	individual exercise
16.	Digital signatures. One-time digital signatures.	individual exercise

2.3.4 Approximate topics of coursework (projects)

Coursework - not provided

2.4 List of educational and methodological support for independent work of students in the discipline

No.	Type of SRS	List of educational and methodological support for the discipline on performing independent work
1	basic concepts And history development informational safety.	Information security: a textbook for university students / S. V. Petrov, I. P. Slinkova, V. V. Gafner, P. A. Kislyakov; Ministry of Education and Science of Russia. Federation, Federal State Budgetary Educational Institution of Higher Professional Education "Novosibirsk State Pedagogical University", Federal State Budgetary Educational Institution of Higher Professional Education "Moscow State Pedagogical University". - Moscow ; Novosibirsk: [ARTA], 2012 Standards for the design of program source code and modern integrated software development environments: educational and methodological manual. Yu.V. Koltsov [etc.] – Krasnodar: Kuban State University, 2017 Financial Cybersecurity Risk Management: Leadership Perspectives and Guidance for Systems and Institutions." 12 Authors: Paul Rohmeyer andJEnnifer L. Bayuk. The book was published in 2018 Managing Financial Cybersecurity Risks: Leadership Perspectives and Recommendations for Systems and Institutions. Authors: Paul Rohmeier and Jennifer L. Bayuk. 2018.
2	final fields. polynomials above finite field. sequences hell is a finite field.	Information security: a textbook for university students / S. V. Petrov, I. P. Slinkova, V. V. Gafner, P. A. Kislyakov; Ministry of Education and Science of Russia. Federation, Federal State Budgetary Educational Institution of Higher Professional Education "Novosibirsk State Pedagogical University", Federal State Budgetary Educational Institution of Higher Professional Education "Moscow State Pedagogical University". - Moscow ; Novosibirsk: [ARTA], 2012 Standard for the design of program source code and modern integrated software development environments: educational and methodological manual. Yu.V. Koltsov [etc. – Krasnodar: Kuban State University, 2017 Financial Cybersecurity Risk Management: Leadership Perspectives and Guidance for Systems and Institutions." 12 Authors: Paul Rohmeyer andJEnnifer L. Bayuk. Books published in 2018 Managing Financial Cybersecurity Risks: A Leadership Perspective Recommendations for Systems and Institutions. Authors: Paul Rohmeier and Jennifer L Bayuk. 2018.
3	replacement numbers. permutation numbers. gamming figures.	Information security: a textbook for university students / S. V. Petrov, I. P. Slinkova, V. V. Gafner, P. A. Kislyakov; Ministry of Education and Science of Russia. Federation, Federal State Budgetary Educational Institution of Higher Professional Education "Novosibirsk State Pedagogical University", Federal State Budgetary Educational Institution of Higher Professional Education "Moscow State Pedagogical University". - Moscow ; Novosibirsk: [ARTA], 2012 Standards for the design of program source code and modern integrated software development environments: educational and methodological manual. Yu.V. Koltsov [etc.] – Krasnodar: Kuban State University, 2017 Financial Cybersecurity Risk Management: Leadership Perspectives and Guidance for Systems and Institutions." 12 Authors: Paul Rohmeyer andJEnnifer L. Bayuk. The book was published in 2018 Managing Financial Cybersecurity Risks: Leadership Perspectives and Recommendations for Systems and Institutions. Authors: Paul Rohmeier and Jennifer L. Bayuk. 2018.
4	local systems encryption.	Information security: a textbook for university students / S. V. Petrov, I. P. Slinkova, V. V. Gafner, P. A. Kislyakov; Ministry of Education and Science of Russia. Federation, Federal State Budgetary Educational Institution of Higher Professional Education "Novosibirsk State Pedagogical University", Federal State Budgetary Educational Institution of Higher Professional Education "Moscow State Pedagogical University". - Moscow ; Novosibirsk: [ARTA], 2012 Standard for the design of program source code and modern integrated software development environments: educational and methodological manual. Yu.V. Koltsov [other] – Krasnodar: Kuban State University, 2017 Financial Cybersecurity Risk Management: Leadership Perspectives and Guidance for Systems and Institutions." 12 Authors: Paul Rohmeyer andJEnnifer L. Bayuk. Books published in 2018 Managing Financial Cybersecurity Risks: A Leadership Perspective Recommendations for Systems and Institutions. Authors: Paul Rohmeier and Jennifer L Bayuk. 2018.

No.	Type of SRS	List of educational and methodological support for the discipline on performing independent work
5	absentee systems encryption.	Information security: a textbook for university students / S. V. Petrov, I. P. Slinkova, V. V. Gafner, P. A. Kislyakov; Ministry of Education and Science of Russia. Federation, Federal State Budgetary Educational Institution of Higher Professional Education "Novosibirsk State Pedagogical University", Federal State Budgetary Educational Institution of Higher Professional Education "Moscow State Pedagogical University". - Moscow ; Novosibirsk: [ARTA], 2012 Standard for the design of program source code and modern integrated software development environments: educational and methodological manual. Yu.V. Koltsov [etc. – Krasnodar: Kuban State University, 2017 Financial Cybersecurity Risk Management: Leadership Perspectives and Guidance for Systems and Institutions." 12 Authors: Paul Rohmeyer andJEnnifer L. Bayuk. Books published in 2018 Managing Financial Cybersecurity Risks: A Leadership Perspective Recommendations for Systems and Institutions. Authors: Paul Rohmeier and Jennifer L Bayuk. 2018.
6	identification. digital signatures.	Information security: a textbook for university students / S. V. Petrov, I. P. Slinkova, V. V. Gafner, P. A. Kislyakov; Ministry of Education and Science of Russia. Federation, Federal State Budgetary Educational Institution of Higher Professional Education "Novosibirsk State Pedagogical University", Federal State Budgetary Educational Institution of Higher Professional Education "Moscow State Pedagogical University". - Moscow ; Novosibirsk: [ARTA], 2012 Standard for the design of program source code and modern integrated software development environments: educational and methodological manual. Yu.V. Koltsov [etc. – Krasnodar: Kuban State University, 2017 Financial Cybersecurity Risk Management: Leadership Perspectives and Guidance for Systems and Institutions." 12 Authors: Paul Rohmeyer andJEnnifer L. Bayuk. Books published in 2018 Managing Financial Cybersecurity Risks: A Leadership Perspective Recommendations for Systems and Institutions. Authors: Paul Rohmeier and Jennifer L Bayuk. 2018.

Educational and methodological materials for independent work of students with disabilities and persons with limited health capabilities (HHI) are provided in forms adapted to the limitations of their health and perception of information:

For people with visual impairments:

– in printed form in enlarged font, – in the form of an electronic document, For persons with hearing impairments:

– in printed form,

– in the form of an electronic document.

For persons with musculoskeletal disorders:

– in printed form,

– in the form of an electronic document,

This list can be specified depending on the student population.

3. Educational technologies.

In accordance with the requirements of the Federal State Educational Standard, the discipline program provides for the use of the following educational technologies in the educational process: lecturing using multimedia technologies; small group method, analysis of practical problems and cases.

The following educational technologies are used during training:

− Communication learning technology – aimed at developing communicative competence of students, which is basic, necessary for adaptation to modern conditions of intercultural communication.

− Technology of multi-level (differentiated) training – involves carrying out cognitive activities of students taking into account their individual abilities, capabilities and interests, encouraging them to realize their creative potential. The creation and use of diagnostic tests is an integral part of this technology.

− Modular learning technology – provides for the division of content disciplines into fairly autonomous sections (modules) integrated into the general course.

− Information and communication technologies (ICT) - expanding the scope educational process, increasing its practical orientation, contribute to the intensification of independent work of students and increase cognitive activity. Within the framework of ICT, there are 2 types of technologies:

− Technology of using computer programs - allows you to effectively complement the language learning process at all levels.

− Internet technologies – provide ample opportunities for searching information, development of scientific projects, conducting scientific research.

− Technology of individualization of learning - helps to implement a person-centered approach, taking into account the individual characteristics and needs of students.

− Project technology – focused on modeling social interaction of students in order to solve a problem that is determined within the framework of professional training, highlighting one or another subject area.

− Collaborative learning technology – implements the idea of mutual learning, exercising both individual and collective responsibility for solving educational problems.

− Game technology – allows you to develop skills in considering a number of possible ways to solve problems, activating students' thinking and revealing the personal potential of each student.

− Technology for the development of critical thinking – contributes to the formation a versatile personality capable of thinking critically about information, the ability to select information to solve a given problem.

The integrated use of all the above technologies in the educational process stimulates personal and intellectual activity, develops cognitive processes, and contributes to the formation of competencies that a future specialist should have.

The main types of interactive educational technologies include: − work in small groups (teams) - joint activities of students in a group under the guidance of a leader, aimed at solving a common problem through creative addition

the results of individual work of team members with the division of powers and responsibilities;

− design technology - individual or collective selection activities, distribution and systematization of material on a specific topic, as a result of which a project is compiled;

− analysis of specific situations - analysis of real problem situations that occurred in the relevant field of professional activity, and search for options for the best solutions;

− development of critical thinking – educational activities aimed at development in students of intelligent, reflective thinking, capable of putting forward new ideas and seeing new possibilities.

The approach of analyzing specific tasks and situations is widely used by both teachers and students during lectures, laboratory classes and analysis of the results of independent work. This is due to the fact that when studying and solving each specific problem, there are, as a rule, several methods, and this requires analysis and assessment of a whole set of specific situations.

Topics, assignments and questions for independent work are designed to develop information search skills, the ability to independently expand and deepen the knowledge acquired during lectures and practical classes.

The case study approach is widely used by both teachers and students when analyzing the results of independent work.

For persons with disabilities, consultations can be organized using e-mail.

For people with visual impairments:

– in printed form in enlarged font, – in the form of an electronic document. For people with hearing impairments:

– in printed form,

– in the form of an electronic document.

For persons with musculoskeletal disorders:

– in printed form,

– in the form of an electronic document.

For persons with disabilities, consultations can be organized using e-mail.

This list can be specified depending on the student population.

4. Assessment tools for ongoing monitoring of progress and intermediate certification.

4.1 Fund of assessment funds for ongoing monitoring.

Individual tasks (executed students independently and provided in writing).

1. DES algorithm. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.
2. Algorithm A5. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.
3. Feal algorithm. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.
4. Crypto1 algorithm. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.

5.AlgorithmIDEA. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the Dragon algorithm. Implemented as a software application with a window interface.

6.GOST algorithm94. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.

7.AlgorithmMickey. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the Safer64 algorithm. Implemented as a software application with a window interface.

8.AlgorithmMosquito. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the RC5-64 algorithm. Implemented as a software application with a window interface.

9.AlgorithmRabbit Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.

10. AlgorithmLoki 91. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the RC4 algorithm. Implemented as a software application with a window interface.

eleven. AlgorithmCAST256. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.

12. AlgorithmSEAL. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.

13. AlgorithmAES. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.

14. AlgorithmGMR. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.

15. AlgorithmWake. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.

16. AlgorithmTrivium. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.

17. AlgorithmSkipjack. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.

18. AlgorithmVest. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.

19. AlgorithmFrog. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.

20. AlgorithmVMPC. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.

21. AlgorithmSerpent. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.

22. AlgorithmOryx. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.

23. AlgorithmTEA. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.

24. AlgorithmSalsa20. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.

25. AlgorithmMars. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.

26. AlgorithmMugi. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.

27. AlgorithmBlowfish. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.

28. AlgorithmPike. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.

29.GOST algorithm2012. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.

thirty. AlgorithmDSA. Describe the NP-hard problems underlying the algorithm. Cryptographic strength of the algorithm. Implemented as a software application with a window interface.

4.2 Fund of assessment funds for intermediate certification.

Questions for intermediate certification based on the results of mastering the discipline:

1. Group. Subgroup.
2. Group of productions.
3. Ring. Ideals. Deduction classes.
4. Polynomial rings.
5. End fields.
6. Ring of deductions.
7. Algorithms for multiplication, inversion, calculation of gcd.
8. Extracting roots in a finite field.
9. Calculation of the Jacobi symbol. Simplicity check.
10. Basic concepts and definitions of cryptographic information protection.
11. Encryption.
12. Authentication.
13. RSA system. Deterministic decomposition methods.
14. RSA system. Probabilistic decomposition methods.
15. Discrete logarithm in a finite field. Diffie-Hellman problem.
16. Public key encryption for a group of computable order.
17. Public key encryption for a group of hard-to-compute order.
18. Digital signature on a group of difficult-to-compute order.
19. Digital signature on a group of computable order.
20. Bit presentation schemes. Cryptographic zero-knowledge proof protocols.
21. Cryptographic transmission protocols information from erasing. Cryptographic secret sharing protocol.
22. Cryptographic key management protocols. Timestamp.

23. Basic concepts of classical cryptography. Substitution and permutation ciphers. Block ciphers.
24. Encryption modes.
25. DES cipher.
26. FEAL code.
27. IDEA code.
28. Code GOST 28147-89.
29. Cipher RC5.
30. Blowfish cipher.
31. SAFER code.
32. AES cipher.
33. MD5 cipher.
34. Code GOST R 34.11-94.
35. Hash function. Hashing.

Evaluation criterion:

Grade		
Satisfactorily	**Fine**	**Great**
• If student indicated direction of solving the problem and received “satisfactory” on two questions • If student right decided task; received "good" or "excellent" according to answer at least one question	• if the student is generally correct solved the problem and got “good” on two questions • if the student generally solved the problem correctly and received “satisfactory” for one question and “excellent” for at least one question	• if the student decided correctly task and received a “good” on at least one question and "excellent" in another way

An “unsatisfactory” rating is given if it is impossible to give a “Satisfactory”, “Good”, “Excellent” rating.

Assessment tools for disabled people and persons with limited health capabilities are selected taking into account their individual psychophysical characteristics.

– if necessary, for disabled people and persons with disabilities due to health conditions, additional time is provided to prepare an answer for the exam;

– during the procedure for assessing learning outcomes disabled people and persons with limited health capabilities are provided with the use of technical means necessary for them in connection with their individual characteristics;

– if necessary for students with disabilities

health and disability capabilities, the procedure for assessing learning outcomes in a discipline can be carried out in several stages.

The procedure for assessing the learning outcomes of people with disabilities and people with limited health capabilities in the discipline provides for the provision of information in forms adapted to the limitations of their health and perception of information:

For people with visual impairments:

– in printed form in enlarged font, – in electronic form document.

For people with hearing impairments:

– in printed form,

– in the form of an electronic document.

For persons with musculoskeletal disorders:

– in printed form,

– in the form of an electronic document.

This list can be specified depending on the student population.

5. List of basic and additional educational literature required for mastering the discipline.

5.1 Basic literature:

1. Prokhorova, O.V. Information security and information protection: textbook /

O.V. Prokhorova; Ministry of Education and Science of the Russian Federation, Federal State Budgetary Educational Institution of Higher Professional Education "Samara State University of Architecture and Civil Engineering". - Samara: Samara State University of Architecture and Civil Engineering, 2014. -

http://biblioclub.ru/index.php?page=book&id=438331.

2. Laponina, O.R. Cryptographic foundations of security / O.R. Laponina. - Moscow: National Open University "INTUIT", 2016.

3. Petrenko, V.I. Theoretical foundations of information security: textbook / V.I. Petrenko; Ministry of Education and Science of the Russian Federation, Federal State Autonomous Educational Institution of Higher Professional Education "North Caucasus Federal University". - Stavropol: NCFU, 2015. –

https://biblioclub.ru/index.php?page=book_red&id=458204&sr=1

4. Forouzan, B.A. Mathematics of cryptography and encryption theory / B.A. Forouzan. -

2nd ed., rev. - M.: National Open University "INTUIT", 2016. - https:// biblioclub.ru/index.php?page=book_red&id=428998&sr=1

For mastering the discipline by disabled people and persons with limited health capabilities, there are publications in electronic form in electronic library systems "Lan" and "Jurait".

5.2 Further reading:

1. Basalova, G.V. Fundamentals of cryptography: a course of lectures / G.V. Basalova; National

Open University "INTUIT". - Moscow: Internet University of Information Technologies, 2011. - 253 p. ; The same [Electronic resource]. - URL: http:// biblioclub.ru/index.php?page=book&id=233689 2. Sergeeva, Yu.S.

Data protection. Lecture notes [Electronic resource]: textbook. allowance - Electron. Dan. — Moscow: A-Prior, 2011. — https://biblioclub.ru/index.php?page=book_red&id=72670&sr=1 3. Golikov, A.M.

Information protection in infocommunication systems and networks: textbook / A.M. Golikov; Ministry of Education and Science of the Russian Federation, Tomsk State University of Control Systems and Radioelectronics (TUSUR). - Tomsk: Tomsk State University of Control Systems and Radioelectronics, 2015. – https:// biblioclub.ru/index.php?page=book_red&id=480637&sr=1

4. Dolozov, N.L. Information security software: lecture notes / N.L. Dolozov, T.A. Gultyaeva; Ministry of Education and Science of the Russian Federation, Novosibirsk State Technical University. - Novosibirsk: NSTU, 2015. – https://biblioclub.ru/index.php?page=book_red&id=438307&sr=1

5. Babenko, L.I. Parallel algorithms for solving information security problems / L.I. Babenko, E.A. Ishchukova, I.D. Sidorov. - Moscow: Hot Line Telecom Publishing House, 2014. - https://e.lanbook.com/reader/book/63228/#1.

5.3. Periodicals:

1. Computational methods and programming
2. Mathematical modeling
3. Applied computer science
4. Programming

6. List of resources of the information and telecommunications network “Internet” necessary for mastering the discipline.

1. Purpose and structure encryption algorithms— URL:http://www.ixbt.com/soft/alg-encryption.shtml
2. Cryptographic algorithms used to ensure information security when interacting in

INTERNETURL:http://www.bnti.ru/showart.asp?aid=797&lvl=04.03.07.

7. Guidelines for students on mastering the discipline.

The discipline provides for practical classes in which applied, systematized material is given. During the classes, algorithms and graph representation structures are examined, and examples of developing software applications are provided. After the practical lesson, it is recommended to complete the exercises given in the classroom for independent work.

When students work independently, it is necessary to study the literature listed in the lists above to understand the concepts being introduced, analyze the proposed approaches and methods of program development. When developing a solution to a new problem, a student must be able to select effective and reliable data structures for representing information, select appropriate algorithms for processing them, and take into account the specifics of the programming language in which the implementation will be performed. The student must be able to test and debug problem-solving algorithms in order to detect and eliminate errors in them.

In mastering the discipline by disabled people and persons with limited health capabilities, individual educational work (consultations) is of great importance - additional explanation of the educational material.

Individual consultations on a subject are an important factor contributing to the individualization of learning and the establishment of educational contact between a teacher and a disabled student or person with limited health capabilities.

8. List of information technologies used in implementation educational process in the discipline.

8.1 List of information technologies.

– Checking homework and counseling via email.

– Use of electronic presentations when conducting practical classes.

8.2 List of required software.

– C++ language compiler (“MicrosoftVisualStudio 12”).

– Programs for demonstrating and creating presentations (“Microsoft PowerPoint”). – Programs that support OLE servers (“MicrosoftWord”, “MicrosoftExcel”).

8.3 List of information help systems:

1. Legal reference system “Consultant Plus”
(http://www.consultant.ru)
2. Electronic library system eLIBRARY.RU
(http://www.elibrary.ru)/

9. Material and technical base necessary for implementation educational process in the discipline.

No.	Type of work	Logistical support for discipline and equipment
1.	Lecture classes	Audience, staffed specialized furniture and technical teaching aids
2.	Laboratory exercises	Audience, staffed specialized furniture And technical teaching aids, computers, projector, MS software Windows MicrosoftVisualStudio 12, MicrosoftPowerPoint, MicrosoftWord, MicrosoftExcel
3.	Current control, intermediate certification	Audience, staffed specialized furniture And technical teaching aids, computers, MS Windows software, MicrosoftVisualStudio 12, Microsoft PowerPoint, Microsoft Word, Microsoft Excel
4.	Independent Job	An office for independent work, equipped with computer equipment with the ability to connect to the Internet, a screen enlargement program and provided with access to the electronic information and educational environment of the university.