Министерство образования и науки Российской Федерации Федеральное государственное автономное образовательное учреждение высшего образования «СЕВЕРО-ВОСТОЧНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ имени М. К. АММОСОВА»

Институт математики и информатики Кафедра информационных технологий

	ВЕРЖДАЮ ректор ИМИ		
		/В.И.	Афанасьева /
«	»	20	Γ.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ОД.1.4 – Математические основы защиты информации

для программы магистратуры по направлению подготовки 09.04.01 – Информатика и вычислительная техника

ОДОБРЕНО	ОДОБРЕНО	РЕКОМЕНДОВАНО		
Заведующий кафедрой	Заведующий выпускаю-	Нормоконтроль в составе		
разработчика	щей кафедрой ИТ	ОП пройден		
/	//	/		
Протокол № от	Протокол № от	Протокол № от		
«» 20 г.	«» 20 г.	«» 20 г.		

1. АННОТАЦИЯ

к рабочей программе дисциплины Б1.В.ОД.1.4 – Математические основы защиты информации

Трудоемкость 4 з. е.

1.1. Цель освоения и краткое содержание дисциплины

Целью изучения дициплины «Математические основы защиты информации» является: Дать представление о математических основах наиболее значимых алгоритмов, применяемых для защиты информации.

Краткое содержание дисциплины. Шифрование и криптоанализ на простейших примерах. Основы теории информации и кодирования. Делимость и арифметика в кольцах вычетов. Хэширование и односторонние функции. Криптография с открытым ключом..

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

Таблица 1. Перечень планируемых результатов обучения

Планируемые результаты освоения программы	Планируемые результаты
(содержание и коды компетенций)	обучения по дисциплине
ОК-6 : способностью проявлять инициативу, в том	В результате изучения дисци-
числе в ситуациях риска, брать на себя всю полноту	плины обучающийся должен:
ответственности,	знать: принципы работы ал-
ОПК-1 : способностью воспринимать математи-	горитмов Диффи-Хеллмана и
ческие, естественнонаучные, социально-экономиче-	RSA; принципы работы блоч-
ские и профессиональные знания, умением самосто-	ных шифров;
ятельно приобретать, развивать и применять их для	уметь: оценивать количество
решения нестандартных задач, в том числе в новой	информации в сообщении
или незнакомой среде и в междисциплинарном кон-	об исходе дискретного ве-
тексте,	роятностного эксперимента;
ОПК-5: владением методами и средствами получе-	объяснять разницу между
ния, хранения, переработки и трансляции информа-	симметричными и асиммет-
ции посредством современных компьютерных техно-	ричными криптосистемами;
логий, в том числе в глобальных компьютерных се-	оценивать надежность систе-
тях,	мы при помощи теоретико-
ПК-7: применением перспективных методов иссле-	сложностных оценок
дования и решения профессиональных задач на ос-	владеть навыками: примене-
нове знания мировых тенденций развития вычисли-	ния и реализации основных
тельной техники и информационных технологий	эффективных теоретико-чис-
	ловых алгоритмов, включая
	нахождение НОД, арифметику
	в кольцах вычетов, нахож-
	дение обратного и степени
	вычета mod p .

1.3. Место дисциплины в структуре образовательной программы

Таблица 2. Содержательно-логические связи дисциплины

Индекс	Наименование	Коды учебных дисциплин, практик			
дисциплины	дисциплины	на которые опирается	для которых		
		содержание	содержание		
		дисциплины	дисциплины выступает		
			опорой		
Б1.В.ОД.1.4	Математические	Б1.Б.3.2 – Современные	Б1.В.ДВ.4.2 – Сетевое		
	основы защиты	проблемы информатики	администрирование		
	информации	и вычислительной тех-			
		ники			

1.4. Язык преподавания

Русский.

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

Таблица 3. Выписка из учебного плана

Код и название дисциплины по учебному плану	Б1.В.ОД.1.4 – Математические		
	основы защиты информации		
Курс изучения		1	
Семестр(ы) изучения		2	
Форма промежуточной аттестации (зачет/экзамен)	экза	имен	
Курсовой проект / курсовая работа (указать вид ра-			
боты при наличии в учебном плане), семестр вы-			
полнения			
Трудоемкость (в ЗЕТ)	4 ((4)	
Трудоемкость (в часах) (сумма строк №1, 2, 3),	14	44	
В Т. Ч.:			
№ 1. Контактная работа обучающихся с препо-	Объем	В т. ч.	
давателем (КР), в часах:	аудиторной	с применением	
	работы, в часах	ДОТ или ЭО,	
		в часах	
Объем работы (в часах) (1.1.+1.2.+1.3.)	55		
1.1. Занятия лекционного типа (лекции)	10		
1.2. Занятия семинарского типа, всего, в т.ч.:			
- семинары (практические занятия, коллоквиумы	_		
ит.п.)			
- лабораторные работы	40		
- практикумы			
1.3. КСР (контроль самостоятельной работы, кон-	5		
сультации)			
№ 2. Самостоятельная работа обучающихся	5	3	
(СРС) (в часах)			
№ 3. Количество часов на экзамен (при нали-	3	6	
чии экзамена в учебном плане)			

3. Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий

3.1. Распределение часов по темам и видам учебных занятий

Таблица 4

			I	Контакт	ная ј	работ	а, в	часах	X		
Тема	Всего часов	Лекции	из них с прим-м ЭО и ДОТ	Семинары (практические занятия, коллоквиумы)	из них с прим-м ЭО и ДОТ	Лабораторные работы	из них с прим-м ЭО и ДОТ	Практикумы	из них с прим-м ЭО и ДОТ	КСР (консультации)	Часы СРС
Тема 1. Шифрование и	23	2	0	0	0	8	0	0	0	1	12
криптоанализ на простейших											
примерах											
Тема 2. Основы теории	17	1	0	0	0	8	0	0	0	1	7
информации и кодирования											
Тема 3. Делимость и	23	2	0	0	0	8	0	0	0	1	12
арифметика в кольцах вычетов											
Тема 4. Хэширование и	21	1	0	0	0	8	0	0	0	1	11
односторонние функции											
Тема 5. Криптография с	24	4	0	0	0	8	0	0	0	1	11
открытым ключом											
ВСЕГО ЧАСОВ	108	10	0	0	0	40	0	0	0	5	53

3.2. Содержание тем программы дисциплины

Тема 1. Шифрование и криптоанализ на простейших примерах

Шифр Цезаря, шифры простой замены, полиалфавитные шифры. Частотный анализ. Однократная лента, шифр Вернама.

Тема 2. Основы теории информации и кодирования

Основы теории информации. Энтропия Шеннона. Элементы теории кодирования. Коды Хэмминга. Код Хаффмена.

Тема 3. Делимость и арифметика в кольцах вычетов

НОД и НОК. Алгоритм Евклида. Простые числа, основная теорема арифметики, бесконечность множества простых чисел, распределение простых чисел, числа Мерсенна. Кольцо вычетов Z_m , поле вычетов Z_p . Китайская теорема об остатках. Малая теорема Ферма и теорема Эйлера. Первообразные корни и проблема дискретного логарифма. Алгоритмы генерации псевдослучайных чисел.

Тема 4. Хэширование и односторонние функции

Хэширование. Односторонние функции. Коллизии. Ассоциативные массивы, примеры в различных языках программирования. Алгоритмы MD5, SHA.

Тема 5. Криптография с открытым ключом

Понятие криптографического протокола. Симметричные схемы, проблема обмена ключами. Протокол RSA. Протокол Диффи-Хеллмана. Атаки стороннего канала. Цифровая подпись, применение различных криптосистем для создания цифровой подписи. Понятие об инфраструктуре цифровых подписей. Общая схема SSL/TLS. Понятие о криптографии на эллиптических кривых.

3.3. Формы и методы проведения занятий, применяемые учебные технологии

При проведении занятий и организации СРС используются традиционные технологии сообщающего обучения, предполагающие передачу информации в готовом виде: проведение лекционных занятий, самостоятельная работа с источниками. Предусмотрено использование активных и интерактивных форм обучения с целью формирования и развития профессиональных навыков студентов - выполнение практических работ с применением компьютерных технологий.

4. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

№	Наименование	Вид СРС	Трудо-	Формы и
	раздела (темы)		емкость	методы
	дисциплины		(B	контроля
			часах)	_
1	Шифрование и	Прохождение разделов	12	Предъявление
	криптоанализ на	Ancient Cryptography и		веб-страницы с
	простейших	Ciphers онлайн-курса Journey		информацией о
	примерах	into Cryptography на сайте		прохождении
		Khan Academy		курса.
2	Основы теории	Решение задач	7	Сдача индиви-
	информации и			дуальных
	кодирования			заданий
3	Делимость и	Решение задач	12	Сдача индиви-
	арифметика в кольцах			дуальных
	вычетов			заданий
4	Хэширование и	Написание программ	11	Сдача программ
	односторонние			
	функции			
5	Криптография с	Прохождение раздела Modern	11	Предъявление
	открытым ключом	Cryptography онлайн-курса		веб-страницы с
		Journey into Cryptography на		информацией о
		сайте Khan Academy		прохождении
				курса.
	ИТОГО		53	

5. Методические указания для обучающихся по освоению дисциплины

В связи с небольшим объемом аудиторных часов, важное значение в освоении дисциплины имеет самостоятельная работа. Она предполагает в том числе и сдачу частей онлайнкурсов на английском языке. Это требует самостоятельности и ответственности.

В диагностическом разделе дисциплины приведены тесты по каждому модулю дисци-

плины, которые необходимо выполнить для закрепления теоретических знаний.

Последовательное и добросовестное изучение курса является основой для выработки углубленного понимания важности и проблем защиты информации в областях деятельности, предполагаемых стандартом подготовки по направлению «Информатика и вычислительная техника».

Рейтинговый регламент по дисциплине

Вид выполняемой учебной работы (контролирующие	Количество	Количество
мероприятия)	баллов	баллов
	(min)	(max)
Посещаемость	3	6
Домашние задания, онлайн курсы	16	22
Индивидуальные задания	16	22
Тестирование	10	20
Количество баллов для допуска к экзамену	45	70

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

6.1. Показатели, критерии и шкала оценивания

освоения мых компетенций ОК-6, Знать: принципы работы алгоритопК-15, ПК-7 принципы работы блочных шифров; уметь: опенивать количество информации в сообщении об исходе дискретного вероятностного эксперимента; объяснять разницу между симметричными и асимметричными криптосистемами; оценивать надежность системы при помощи теоретикосложностных оценов валадеть навыками: применения и реализации основных эффективных теоретико-числовых алгоритмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod р. освоения вособен выполнять отлично все задачи из следующего списка: паписать на языке программирования релизацию алгоритма (ведумента) добажно уравнение вида ах + by = c; находить остаток большой степени числа по небольшому модулю, пользуясь теоремами Ферма и Эйлера; определять количество информации, содержащейся в сообщении о конкретном исходе дискретного вероятностного эксперимента; объяснять идеи криптованлиза шифров простой замены и полиалфавитного пифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; базовый не способен выполнить не более одного пункта из вышеперечислен-	Коды	Показатель оценивания	Уровни	Критерий оценивания	Оценка
компетенций ОК-6, ОПК-1, ОПК-5, Принципы работы алгоритмов Диффи-Хеллмана и RSA; принципы работы блочных пиифров; умсть: оценивать количество информации в сообщении об исходе дискретного вероятностного эксперимента; объяснять разницу между симметричными и асимметричными криптосистемами; опјенивать надежность системы при помощи теоретико-сложностных оценов владеть навыками: применения и реализации основных эффективных теоретико-числовых алгоритмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod р. Высокий способен выполнять вее задачи из следующего списка: написать на языке программирования редлизации оалгоритма Евклида; решить диофантов уравнение вида ах + by = c; находить остаток большой степени числа по небольшому модулю, пользуясь теоремами Ферма и Эйлера; определять количество информации, содержащейся в сообщении о конкретном исходе дискретного вероятностного эксперимента; объяснять идеи криптоанализа шифров простой замены и полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации е надежностью криптосистем открытгог ключа; базовый не способен выполнить корпитосистем открытгого ключа; то долем открытгого ключа; то долем открытгого ключа; то способен выполнить корпитосистем открытгого ключа; то долем открытгого ключа; то долем открытгого ключа; то способен выполнить корпитосистем открытгого ключа; то долем от долем открытело ключа; то долем открытело ключа; то долем от доле	оценива-	(дескриптор) (по п.1.2)	освоения		
ОК-6, ОПК-1, ОПК-5, ПК-7 принципы работы алгорит- ОПК-5, ПК-7 принципы работы блочных шифров; уметь: оценивать количество информации в сообщении об исходе дискретного вероятностного эксперимента; объяснять разницу между симметричными криптосистемами; оценивать надежность системы при помощи теоретико- сложностных оценок владеть навыками: применения и реализации основных эффективных теоретико-числовых алторитмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod р. Телем объяснять идежность системами; оценивать надежность осистемы при помощи теоретико- сложностных оценок владеть навыками: применения и реализации основных эффективных теоретико-числовых алторитмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod р. Телем объяснять идем криптованиза шифров простой замены и полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытгого ключа; Телем объяснять в шполинть по принцення из вышеперечислены выполнить на более одного пункта из вышеперечислень	емых				
ОК-6, OПК-1, OПК-1, OПК-5, OПК-5, OПК-5, OПК-5, OПК-5, OПК-7 знать: принципы работы алгоритим вы высокий принципы работы блочных пифров; уметь: оценивать количество информации в сообщении об исходе дискретного вероятностного эксперимента; объяснять разницу между симметричными и асимметричными криптосистемами; оценивать надежность системы при помощи теоретикосложностных оценов владеть навыками: применения и реализации основных эффективных теоретико-числовых алгоритмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod p . высокий высокий вес задачи из следующего списка: написать на языке программирования релизацию алгоритма Евклида; решить диофантово уравнение вида $ax + by = c$; находить остаток большой степени числа по небольшому модулю, пользуясь теоремами Ферма и Эйлера; определять количество информации, содержащейся в сообщении о конкретном исходе дискретного вероятностного эксперимента; объяснять цдеи криптоанализа шифров простой замены и полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытгого ключа; базовый пестособен выполнить не более одного пункта из вышеперечислен- хорошо неостанующей списка: написать на языке программирования релизицию алгоритма Евклида; решить диофантово уравнение вида $ax + by = c$; находить остаток большой, степени числа по небольшому модулю, пользуясь теоремами Ферма и Эйлера; определять сообщения о конкретном исходе дискретного вероятностного эксперимента; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа;					
ОПК-1, ОПК-5, ПВИ-17 припципы работы алгоритмов Диффи-Хеллмана и RSA; принципы работы блочных шифров; уметь: оценивать количество информации в сообщении об исходе дискретного вероятностного эксперимента; объяснять разнищу между симметричными криптосистемами; оценивать надежность системы при помощи теоретикосложностных оценок владеть навыками: применения и реализации основных эффективных теоретико-числовых алгоритмов, включая нахождение НОД, арифметику в кольщах вычетов, нахождение обратного и степени вычета mod р. Все задачи из следующего списка: написать на языке программирования релизацию алгоритма Евклида; решить диофантово уравнение вида $ax + by = c$; находить остаток большой степени числа по небольшому модулю, пользуясь теоремами Ферма и Эйлера; определять количество информации, содержащейся в сообщении о конкретном исходе дискретного вероятностного эксперимента; объяснять идеи криптоанализа шифров простой замены и полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; не способен выполнить не более одного пункта из вышеперечислен-					
ОПК-5, ПК-7 принципы работы блочных шифров; умсть: оценивать количество информации в сообщении об исходе дискретного веро- ятностного эксперимента; объяснять разницу между симметричными и асимметричными криптосистемами; оценивать надежность системы при помощи теоретикосложностных оценок владеть навыками: применения и реализации основных эффективных теоретико-числовых алгоритмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение ного и степени вычета mod p . ОПК-5, принципы работы блочных шиформации доновных эффективных теоретико-числовых алгоритмов, включая нахождение нОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod p .		l 	высокий	способен выполнять	отлично
ПК-7 принципы работы блочных шифров; уметь: опенивать количество информации в сообщении об исходе дискретного вероятностного эксперимента; объяснять разницу между симметричными и асимметричными криптосистемами; оценивать надежность системы при помощи теоретикосложностных оценов владеть навыками: применения и реализации основных эффективных теоретико-числовых алгоритмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod p . написать на языке программирования релизации однования объяснять разницу адмофантово уравнение вида $ax + by = c$; находить остаток большой степени числа по небольшому модулю, пользуясь теоремами Ферма и Эйлера; определять количество информации, содержащейся в сообщении о конкретном исходе дискретного вероятностного эксперимента; объяснять идеи криптоанализа шифров простой замены и полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; не способен выполнить ие более одного пункта из вышеперечислен-				все задачи из	
программирования релизацию алгоритма Евклида; решить диофантово уравнение вида $ax + by = c$; находить остаток большой степени числа по небольшому симметричными и асимметричными криптосистемами; ощенивать надежность системы при помощи теоретикосложностных оценок владеть навыками: применения и реализации основных эффективных теоретико-числовых алгоритмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod p . применения вычета mod p . программирования релизацию алгоритма Евклида; решить диофантово уравнение вида $ax + by = c$; находить остаток большой степени числа по небольшому модулю, пользуясь теоремами Ферма и Эйлера; определять количество информации, содержащейся в сообщении о конкретном исходе дискретного вероятностного эксперимента; объяснять идеи криптоанализа шифров простой замены и полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого кпюча; те сообен выполнить не более одного пункта из вышеперечислен-				следующего списка:	
уметь: оценивать количество информации в сообщении об исходе дискретного вероятностного эксперимента; объясиять разницу между симметричными и асимметричными криптосистемами; оценивать надежность системы при помощи теоретикосложностных оценок владеть навыками: применения и реализации основных эффективных теоретико-числовых алгоритмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod p . релизациио алгоритма E Бклида; решить диофантово уравнение вида $ax + by = c$; находить остепени числа по небольшому модулю, пользуясь теоремами Ферма и Эйлера; определять количество информации, содержащейся в сообщении о конкретном исходе дискретного вероятностного эксперимента; объяснять идеи криптоанализа шифров простой замены и полиалфавитного шифра; объясиять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; не способен выполнить не более одного пункта из вышеперечислен-	ПК-7	* *		написать на языке	
оценивать количество информации в сообщении об исходе дискретного вероятностного эксперимента; объясиять разницу между симметричными к риптосистемами; оценивать надежность системы при помощи теоретикосложностных оценок владеть навыками: применения и реализации основных эффективных теоретико-числовых алгоритмов, включая нахождение НОД, арифметику в кольщах вычетов, нахождение обратного и степени вычета mod p . Вакина денивать надежность системование информации, содержащейся в сообщении о конкретном исходе дискретного эксперимента; объяснять идеи криптоанализа шифров простой замены и полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; базовый не способен выполнить не более одного пункта из вышеперечислен-		шифров;		программирования	
формации в сообщении об исходе дискретного вероятностного эксперимента; объяснять разницу между симметричными и асимметричными криптосистемами; оценивать надежность системы при помощи теоретикосложностных оценок владеть навыками: применения и реализации основных эффективных теоретико-числовых алгоритмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod p . формации, содержащейся в сообщении о конкретном исходе дискретного вероятностного эксперимента; объяснять идеи криптоанализа шифров простой замены и полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; базовый не способен выполнить не более одного пункта из вышеперечислен-		уметь:		релизацию алгоритма	
исходе дискретного веро- ятностного эксперимента; объяснять разницу между симметричными и асиммет- ричными криптосистемами; оценивать надежность систе- мы при помощи теоретико- сложностных оценок владеть навыками: применения и реализации основных эффективных теоретико-числовых алго- ритмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod p . вида $ax + by = c$; находить остаток большой степени числа по небольшому модулю, пользуясь теоремами Ферма и Эйлера; определять количество информации, содержащейся в сообщении о конкретном исходе дискретного вероятностного эксперимента; объяснять идеи криптоанализа шифров простой замены и полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; базовый не способен выполнить не более одного пунк- та из вышеперечислен-		оценивать количество ин-		Евклида; решить	
ятностного эксперимента; объяснять разницу между симметричными и асимметричными криптосистемами; оценивать надежность системы при помощи теоретикоссложностных оценок владеть навыками: применения и реализации основных эффективных теоретико-числовых алгоритмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod р. Валадеть навыками: применения и реализации основных эффективных теоретико-числовых алгоритмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod р. Валадеть навыками: применения и реализации с количество сообщении о конкретном исходе дискретного вероятностного эксперимента; объяснять идеи криптоанализа шифров простой замены и полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; базовый не способен выполнить не более одного пункта из вышеперечислен-		формации в сообщении об		диофантово уравнение	
объяснять разницу между симметричными и асимметричными и асимметричными криптосистемами; оценивать надежность системы при помощи теоретикосложностных оценок владеть навыками: применения и реализации основных эффективных теоретико-числовых алгоритмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod р.		исходе дискретного веро-		вида $ax + by = c$;	
симметричными и асимметричными криптосистемами; оценивать надежность системы при помощи теоретикосложностных оценок владеть навыками: применения и реализации основных эффективных теоретико-числовых алгоритмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod р. Вазовый по небольшому модулю, пользуясь теоремами Ферма и Эйлера; определять количество информации, содержащейся в сообщении о конкретном исходе дискретного вероятностного эксперимента; объяснять идеи криптоанализа шифров простой замены и полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; не способен выполнить не более одного пункта из вышеперечислен-		ятностного эксперимента;		находить остаток	
ричными криптосистемами; оценивать надежность системы при помощи теоретикосложностных оценок владеть навыками: применения и реализации основных эффективных теоретико-числовых алгоритмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod р. Воличество информации, содержащейся в сообщении о конкретном исходе дискретного вероятностного эксперимента; объяснять идеи криптоанализа шифров простой замены и полиалфавитного шифра, объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; не способен выполнить не более одного пункта из вышеперечислен-		объяснять разницу между		большой степени числа	
оценивать надежность системы при помощи теоретико- сложностных оценок владеть навыками: применения и реализации основных эффективных теоретико-числовых алго- ритмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod p. Вастивных теоремами Ферма и Эйлера; определять количество информации, содержащейся в сообщении о конкретном исходе дискретного вероятностного эксперимента; объяснять идеи криптоанализа шифров простой замены и полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; базовый не способен выполнить не более одного пункта из вышеперечислен-		симметричными и асиммет-		по небольшому	
мы при помощи теоретико- сложностных оценок владеть навыками: применения и реализации основных эффективных теоретико-числовых алго- ритмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod р. враина вычета тобратного и степени вычета тобратностного и степени вычета тобратностного и степени вычета тобратностного и простой замены и полиалфавитного и проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; базовый не способен выполнить не более одного пункта из вышеперечисленного и степени выполнить не более одного пункта из вышеперечисленного и степени вычета тобратностного и простой замены и полиалфавитного и проблем дискретного логарифма и факторизации с надежностью криптосистем открытосистем открытос		ричными криптосистемами;		модулю, пользуясь	
сложностных оценок владеть навыками: применения и реализации основных эффективных теоретико-числовых алго- ритмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обрат- ного и степени вычета mod р. количество информации, содержащейся в сообщении о конкретном исходе дискретного вероятностного эксперимента; объяснять идеи криптоанализа шифров простой замены и полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; базовый не способен выполнить не более одного пунк- та из вышеперечислен-		оценивать надежность систе-		теоремами Ферма и	
владеть навыками: применения и реализации основных эффективных теоретико-числовых алгоритмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod р. вероятностного эксперимента; объяснять идеи криптоанализа шифров простой замены и полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; базовый не способен выполнить не более одного пункта из вышеперечислен-		мы при помощи теоретико-		Эйлера; определять	
применения и реализации основных эффективных теоретико-числовых алгоритмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod р. Воторитмов, включая нахождение ного и степени вычета mod р. Воторитмов, включая нахождение обратного и степени вычета mod р. Воторитмов, включая нахождение обратного и степени вычета mod рактерия и полиализа шифров простой замены и полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; Воторитмов, включая нахождение обратного и степени вычета mod рактерия и полиалфавитного		сложностных оценок		количество	
основных эффективных теоретико-числовых алгоритмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod р. Видение обратного и степени вычета mod р. Видение обратного и степени вычета теоритеов, нахождение обратного и степени вычета теоритеов, простой замены и полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; Базовый не способен выполнить не более одного пункта из вышеперечислен-		владеть навыками:		информации,	
теоретико-числовых алгоритмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod р. конкретном исходе дискретного вероятностного эксперимента; объяснять идеи криптоанализа шифров простой замены и полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; базовый не способен выполнить хорошо не более одного пункта из вышеперечислен-		применения и реализации		содержащейся в	
ритмов, включая нахождение НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod р. Вероятностного эксперимента; объяснять идеи криптоанализа шифров простой замены и полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; базовый не способен выполнить не более одного пункта из вышеперечислен-		основных эффективных		сообщении о	
НОД, арифметику в кольцах вычетов, нахождение обратного и степени вычета mod р. Вероятностного эксперимента; объяснять идеи криптоанализа шифров простой замены и полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; базовый не способен выполнить не более одного пункта из вышеперечислен-		теоретико-числовых алго-		конкретном исходе	
вычетов, нахождение обратного и степени вычета mod р. эксперимента; объяснять идеи криптоанализа шифров простой замены и полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; базовый не способен выполнить не более одного пункта из вышеперечислен-		ритмов, включая нахождение		дискретного	
ного и степени вычета mod p. объяснять идеи криптоанализа шифров простой замены и полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; базовый не способен выполнить хорошо не более одного пункта из вышеперечислен-		НОД, арифметику в кольцах		вероятностного	
р. криптоанализа шифров простой замены и полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; базовый не способен выполнить корошо не более одного пункта из вышеперечислен-		вычетов, нахождение обрат-		эксперимента;	
простой замены и полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; базовый не способен выполнить корошо не более одного пункта из вышеперечислен-		ного и степени вычета mod		объяснять идеи	
полиалфавитного шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; базовый не способен выполнить не более одного пунк- та из вышеперечислен-		$\mid p$.		криптоанализа шифров	
шифра; объяснять связь сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; базовый не способен выполнить хорошо не более одного пункта из вышеперечислен-				простой замены и	
сложности проблем дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; базовый не способен выполнить хорошо не более одного пункта из вышеперечислен-				полиалфавитного	
дискретного логарифма и факторизации с надежностью криптосистем открытого ключа; базовый не способен выполнить хорошо не более одного пункта из вышеперечислен-				шифра; объяснять связь	
и факторизации с надежностью криптосистем открытого ключа; базовый не способен выполнить хорошо не более одного пункта из вышеперечислен-				сложности проблем	
надежностью криптосистем открытого ключа; базовый не способен выполнить хорошо не более одного пункта из вышеперечислен-				дискретного логарифма	
криптосистем открытого ключа; базовый не способен выполнить хорошо не более одного пункта из вышеперечислен-				и факторизации с	
открытого ключа; базовый не способен выполнить хорошо не более одного пункта из вышеперечислен-				надежностью	
базовый не способен выполнить хорошо не более одного пунк- та из вышеперечислен-				криптосистем	
не более одного пунк- та из вышеперечислен-				открытого ключа;	
та из вышеперечислен-			базовый	не способен выполнить	хорошо
				не более одного пунк-	
				та из вышеперечислен-	
HOIO				НОГО	

	мини-	не способен выполнить	удовл
	мальный	не более двух пункта из	
		вышеперечисленного	
	не осво-	не способен выполнить	неудовл
	ено	три или более пунктов	
		из вышеперечисленно-	
		го	

6.2. Типовые контрольные задания (вопросы) для промежуточной аттестации

Коды оценива- емых компе- тенций	Оцениваемый показатель (ЗУВ)	Тема	Образец типового (тестового или практического) задания (вопроса)
ОК-6, ОПК-1, ОПК-5, ПК-7	знать принципы работы алгоритмов Диффи- Хеллмана и RSA	5	Объясните, сколько попыток нужно сделать для полного перебора с целью взлома данной пары RSA
ОПК-1	уметь оценивать количество информации в сообщении об исходе дискретного вероятностного эксперимента	2	Сколько бит информации содержит сообщение о том, что из колоды в 36 карт достали даму пик?
ОК-6, ОПК-1, ОПК-5, ПК-7	уметь объяснять разницу между симметричными и асимметричными криптосистемами	1, 5	Какова роль RSA в ходе установления сессии TLS. Какое шифрование применяется для обмена данными, когда сессия установлена?
ОК-6, ОПК-1, ПК-7	уметь оценивать на- дежность системы при помощи теоретико- сложностных оценок	3, 4	Предположим, найден алгоритм разложения произвольного целого n на множители со сложностью $O(n \log n)$. Что можно будет в таком случае сказать о сложности взлома RSA?
ОПК-1	владеть навыками применения и реализации основных эффективных теоретикочисловых алгоритмов	3	Найдите остаток $22^{3006} \mod 2011$.

Экзаменационные вопросы

- 1. Шифр Цезаря. Шифры простой замены.
- 2. Полиалфавитные шифры. Шифр Виженера. Частотный анализ.
- 3. Однократная лента, шифр Вернама.
- 4. Энтропия Шеннона. Энтропия исходов экспериментов с бросанием кости.
- 5. Коды Хэмминга.
- 6. Код Хаффмена.
- 7. НОД и НОК. Алгоритм Евклида.
- 8. Простые числа, основная теорема арифметики. Кольцо вычетов, поле вычетов. Китайская теорема об остатках.
- 9. Малая теорема Ферма.

- 10. Мультипликативные функции. Функция Эйлера.
- 11. Теорема Эйлера.
- 12. Первообразные корни, проблема дискретного логарифма.
- 13. Алгоритмы генерации псевдослучайных чисел.
- 14. Хэширование и односторонние функции. Коллизии. Ассоциативные массивы, примеры в различных языках программирования.
- 15. Алгоритмы MD5, SHA.
- 16. Алгоритм Диффи–Хеллмана.
- 17. Криптосистема RSA.
- 18. Цифровая подпись, применение различных криптосистем для создания цифровой подписи.
- 19. Криптосистемы на эллиптических кривых.

6.3. Методические материалы, определяющие процедуры оценивания

Форма промежуточной аттестации: экзамен.

Данный вид комплексного испытания предполагает последовательное выполнение всех форм текущего контроля, таких, как тесты, прохождение онлайн-курсов и выполнение практических заданий.

Тестирование. Данная форма контроля направлена на оценку основных теоретических знаний обучающегося по мере освоения основных разделов дисциплины.

Контрольные работы. В этой форме промежуточного контроля проверяются способности обобщенного анализа имеющихся теоретических знаний и умение пользоваться специальной литературой. Во время выполнения контрольной работы по темам 3—5 разрешается пользоваться справочной литературой

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Перечень литературы

№	Автор, название, место издания,	Наличие	НБ СВФУ,	Электронные
	издательство, год издания учебной	грифа, вид	кафедраль-	издания: точка
	литературы, вид и характеристика иных	грифа	ная	доступа к ресурсу
	информационных ресурсов		библиотека	(наименование
			и кол-во	ЭБС, ЭБ СВФУ)
			экземпляров	
	Основная	литература		
1	Элементы теории обыкновенных			ЭБС «Лань»,
	представлений и характеров конечных			режим доступа:
	групп с приложениями в			http://e.lanbook
	криптографии. СПб. : Лань, 2015.			.com/book/65044
2	Бабенко Л. К., Параллельные		1	
	алгоритмы для решения задач защиты			
	информации. М.: Горячая линия-			
	Телеком, 2014			
	Дополнителы	ная литерату	pa	
1	Левин М. PGP: Кодирование и		1	
	шифрование информации с открытым			
	ключом. М: Майор, 2001			
2	Глухов М. М., Круглов И. А., Пичкур			ЭБС «Лань»,
	А. Б., Черемушкин А. В. Введение в			режим доступа:
	теоретико-числовые методы			http://e.lanbook
	криптографии. СПб. : Лань, 2011.			.com/book/1540
3	Кормен Т. Х. Алгоритмы. Вводный		1	
	курс. М.: Вильямс, 2015			

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее сеть-Интернет), необходимых для освоения дисциплины

- 1. Анисимов В. В. Криптографические методы защиты информации. Режим доступа: https://sites.google.com/site/anisimovkhv/learning/kripto
- 2. Лапонина О. Р. Криптографические основы безопасности. Режим доступа: http://www.intuit.ru/studies/courses/28/28/info
- 3. Journey into cryptography. Computer Scence // Khan Academy. Режим доступа: https://www.khanacademy.org/computing/computer-science/cryptography/

9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для проведения лекционных занятий требуется аудитория, оборудованная доской, мультимедийным проектором с экраном. Для проведения лабораторных занятий требуется компьютерный класс с подключением к интернету.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения

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

При осуществлении образовательного процесса по дисциплине используются следующие информационные технологии:

- использование на занятиях электронных изданий (чтение лекций с использованием слайд-презентаций);
- ведение учета посещаемости и выполнения учебных заданий в системе Google Docs;
- разработка обучающимися программ на языках Python и Cu++;
- организация взаимодействия с обучающимися посредством электронной почты, специализированного образовательного форума Piazza;
- компьютерное тестирование.

10.2. Перечень программного обеспечения

При осуществлении образовательного процесса по дисциплине используются следующее программное обеспечение:

- язык Python версии 3 и новее;
- среда разработки JetBrains PyCharm;
- среда разработки Visual Studio;
- интернет-браузер.

ЛИСТ АКТУАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Б1.В.ОД.1.4 — Математические основы защиты информации

Учебный год	Внесенные изменения	Преподаватель (ФИО)	Протокол заседания выпускающей кафедры (дата, номер), ФИО зав.кафедрой, подпись

В таблице указывается только характер изменений (например, изменение темы, списка источников по теме или темам, средств промежуточного контроля) с указанием пунктов рабочей программы. Само содержание изменений оформляется приложением по сквозной нумерации.

Содержание

l	АННОТАЦИЯ	2			
	1.1 Цель освоения и краткое содержание дисциплины	2			
	1.2 Перечень планируемых результатов обучения по дисциплине, соотнесенных				
	с планируемыми результатами освоения образовательной программы	2			
	1.3 Место дисциплины в структуре образовательной программы	3			
	1.4 Язык преподавания	3			
2	Объем дисциплины в зачетных единицах с указанием количества академиче-				
	ских часов, выделенных на контактную работу обучающихся с преподавателем				
	(по видам учебных занятий) и на самостоятельную работу обучающихся	4			
3	Содержание дисциплины, структурированное по темам с указанием отведен-				
	ного на них количества академических часов и видов учебных занятий	5			
	3.1 Распределение часов по темам и видам учебных занятий	5			
	3.2 Содержание тем программы дисциплины	5			
	3.3 Формы и методы проведения занятий, применяемые учебные технологии	6			
4	Перечень учебно-методического обеспечения для самостоятельной работы обу-				
	чающихся по дисциплине	6			
5	Методические указания для обучающихся по освоению дисциплины	6			
6	Фонд оценочных средств для проведения промежуточной аттестации обучаю-				
	щихся по дисциплине	8			
	6.1 Показатели, критерии и шкала оценивания	8			
	6.2 Типовые контрольные задания (вопросы) для промежуточной аттестации	9			
	6.3 Методические материалы, определяющие процедуры оценивания	10			
7	Перечень основной и дополнительной учебной литературы, необходимой для				
	освоения дисциплины	11			
8	Перечень ресурсов информационно-телекоммуникационной сети «Интернет»				
		11			
9	Описание материально-технической базы, необходимой для осуществления об-				
	разовательного процесса по дисциплине	12			
10	Перечень информационных технологий, используемых при осуществлении об-				
	разовательного процесса по дисциплине, включая перечень программного				
		12			
	10.1 Перечень информационных технологий, используемых при осуществлении				
	образовательного процесса по дисциплине	12			
		12			