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

УТВЕРЖДАЮ
Директор ИМИ
_____ / В. И. Афанасьева /

«___» _____ 20___ г.

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 Заведующий кафедрой разработчика _____ /_____/	ОДОБРЕНО Заведующий выпускающей кафедрой ИТ _____ /_____/	РЕКОМЕНДОВАНО Нормоконтроль в составе ОП пройден _____ /_____/
Протокол № __ от «___» _____ 20___ г.	Протокол № __ от «___» _____ 20___ г.	Протокол № __ от «___» _____ 20___ г.

Якутск – 2016

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 диципины «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 (содержание и коды компетенций)	Планируемые результаты обучения по дисциплине
ОК-6 : способностью проявлять инициативу, в том числе в ситуациях риска, брать на себя всю полноту ответственности, ОПК-1 : способностью воспринимать математические, естественнонаучные, социально-экономические и профессиональные знания, умением самостоятельно приобретать, развивать и применять их для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте, ОПК-5 : владением методами и средствами получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе в глобальных компьютерных сетях, ПК-7 : применением перспективных методов исследования и решения профессиональных задач на основе знания мировых тенденций развития вычислительной техники и информационных технологий	В результате изучения дисциплины обучающийся должен: знать: принципы работы алгоритмов Диффи-Хеллмана и RSA; принципы работы блочных шифров; уметь: оценивать количество информации в сообщении об исходе дискретного вероятностного эксперимента; объяснять разницу между симметричными и асимметричными криптосистемами; оценивать надежность системы при помощи теоретико-сложностных 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.

1.3. Место дисциплины в структуре образовательной программы

Таблица 2. *Содержательно-логические связи дисциплины*

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

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)	экзамен	
Курсовой проект / курсовая работа (указать вид работы при наличии в учебном плане), семестр выполнения		
Трудоемкость (в ЗЕТ)	4 (4)	
Трудоемкость (в часах) (сумма строк №1, 2, 3), в т. ч.:	144	
№ 1. Контактная работа обучающихся с преподавателем (КР), в часах:	Объем аудиторной работы, в часах	В т. ч. с применением 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 и т. п.)	–	
- лабораторные работы	40	
- практикумы		
1.3. КСР (контроль самостоятельной работы, консультации)	5	
№ 2. Самостоятельная работа обучающихся (СРС) (в часах)	53	
№ 3. Количество часов на экзамен (при наличии экзамена в учебном плане)	36	

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

Тема	Всего часов	Контактная работа, в часах									Часы СРС
		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)	
Тема 1. Шифрование и криптоанализ на простейших примерах	23	2	0	0	0	8	0	0	0	1	12
Тема 2. Основы теории информации и кодирования	17	1	0	0	0	8	0	0	0	1	7
Тема 3. Делимость и арифметика в кольцах вычетов	23	2	0	0	0	8	0	0	0	1	12
Тема 4. Хэширование и односторонние функции	21	1	0	0	0	8	0	0	0	1	11
Тема 5. Криптография с открытым ключом	24	4	0	0	0	8	0	0	0	1	11
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 раздела (темы) дисциплины	Вид СРС	Трудоемкость (в часах)	Формы и методы контроля
1	Шифрование и криптоанализ на простейших примерах	Прохождение разделов Ancient Cryptography и Ciphers онлайн-курса Journey into Cryptography на сайте Khan Academy	12	Предъявление веб-страницы с информацией о прохождении курса.
2	Основы теории информации и кодирования	Решение задач	7	Сдача индивидуальных заданий
3	Делимость и арифметика в кольцах вычетов	Решение задач	12	Сдача индивидуальных заданий
4	Хэширование и односторонние функции	Написание программ	11	Сдача программ
5	Криптография с открытым ключом	Прохождение раздела Modern Cryptography онлайн-курса Journey into Cryptography на сайте Khan Academy	11	Предъявление веб-страницы с информацией о 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 онлайн-курсов 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 мероприятия)	Количество баллов (min)	Количество баллов (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

Коды оцениваемых компетенций	Показатель оценивания (дескриптор) (по п.1.2)	Уровни освоения	Критерий оценивания	Оценка
ОК-6, ОПК-1, ОПК-5, ПК-7	знать: принципы работы алгоритмов Диффи-Хеллмана и RSA; принципы работы блочных шифров; уметь: оценивать количество информации в сообщении об исходе дискретного вероятностного эксперимента; объяснять разницу между симметричными и асимметричными криптосистемами; оценивать надежность системы при помощи теоретико-сложностных 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.	высокий	способен выполнять 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;	отлично
		базовый	не способен выполнить не более одного пункта из вышеперечисленного	хорошо

		мини-мальный	не способен выполнить не более двух пункта из вышеперечисленного	удовл
		не освоено	не способен выполнить три или более пунктов из вышеперечисленного	неудовл

6.2. Типовые контрольные задания (вопросы) для промежуточной аттестации

Коды оцениваемых компетенций	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 надежность 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 теоретико-числовых 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, издательство, год издания учебной литературы, вид и характеристика иных информационных ресурсов	Наличие грифа, вид грифа	НБ СВФУ, кафедральная библиотека и кол-во экземпляров	Электронные издания: точка доступа к ресурсу (наименование ЭБС, ЭБ СВФУ)
Основная литература				
1	Элементы теории обыкновенных представлений и характеров конечных групп с приложениями в криптографии. СПб. : Лань, 2015.		—	ЭБС «Лань», режим доступа: http://e.lanbook.com/book/65044
2	Бабенко Л. К., Параллельные алгоритмы для решения задач защиты информации. М.: Горячая линия-Телеком, 2014		1	
Дополнительная литература				
1	Левин М. PGP: Кодирование и шифрование информации с открытым ключом. М: Майор, 2001		1	
2	Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В. Введение в теоретико-числовые методы криптографии. СПб. : Лань, 2011.		—	ЭБС «Лань», режим доступа: http://e.lanbook.com/book/1540
3	Кормен Т. Х. Алгоритмы. Вводный курс. М.: Вильямс, 2015		1	

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 Си++;
- 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