

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 выпускаю-
щей кафедрой ИТ

_____ / _____ /

РЕКОМЕНДОВАНО

Нормоконтроль в составе
ОП пройден

_____ / _____ /

Протокол № ____ от

« ____ » _____ 20 ____ г.

Протокол № ____ от

« ____ » _____ 20 ____ г.

Протокол № ____ от

« ____ » _____ 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 освоения дисциплины «Математические основы защиты информации» является

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
ПК-7 : применением перспективных методов исследования и решения профессиональных задач на основе знания мировых тенденций развития вычислительной техники и информационных технологий	

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		

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.:	108	
№ 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.)	49	
1.1. Занятия лекционного типа (лекции)	15	
1.2. Занятия семинарского типа, всего, в т.ч.:		
- семинары (практические занятия, коллоквиумы и т. п.)	–	
- лабораторные работы	34	
- практикумы		
1.3. КСР (контроль самостоятельной работы, консультации)	5	
№ 2. Самостоятельная работа обучающихся (СРС) (в часах)	54	
№ 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)
а	28	28	28	28	28	28	28	28	28	28

3.2. Содержание тем программы дисциплины

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

№	Наименование раздела (темы) дисциплины	Вид СРС	Трудо-емкость (в часах)	Формы и методы контроля
---	--	---------	-------------------------	-------------------------

5. Методические указания для обучающихся по освоению дисциплины

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

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 Максим. 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>

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

[illegible]

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

1	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	2
1.4	Язык преподавания	2
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	3
3	Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий	4
3.1	Распределение часов по темам и видам учебных занятий	4
3.2	Содержание тем программы дисциплины	4
4	Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине	4
5	Методические указания для обучающихся по освоению дисциплины	4
6	Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	4
7	Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	5
8	Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее сеть-Интернет), необходимых для освоения дисциплины	5
9	Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	6
10	Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения	6
10.1	Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине	6
10.2	Перечень программного обеспечения	6