МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Мурманский арктический государственный университет»
(ФГБОУ ВО «МАГУ»)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.О.17.04 Защита информации

(название дисциплины (модуля) в соответствии с учебным планом)

основной профессиональной образовательной программы
по направлению подготовки

01.03.02 Прикладная математика и информатика
направленность (профиль) Управление данными и машинное обучение

(код и наименование направления подготовки
с указанием направленности (наименования магистерской программы))

высшее образование – бакалавриат

уровень профессионального образования: высшее образование – бакалавриат / высшее образование – специалитет, магистратура / высшее образование – подготовка кадров высшей квалификации

бакалавр

квалификация

очная

форма обучения

2021

год набора

Составитель(и):

Крупорницкий Дмитрий Анатольевич
Старший преподаватель кафедры МФиИТ

Утверждено на заседании кафедры
математики, физики и информационных
технологий факультета
математических и естественных наук
(протокол № 07 от 12.04.2021)

Переутверждено на заседании кафедры
математики, физики и информационных
технологий факультета
математических и естественных наук
(протокол № 09 от 02.07.2021)

Зав. кафедрой _____ Лазарева И.М.
подпись Ф.И.О.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ) – Данный курс знакомит студентов с основными средствами и методами, обеспечивающими информационную безопасность. Особое внимание уделяется криптографическим методам защиты информации, а именно: криптосистемам с секретным ключом (симметричным криптоалгоритмам) и криптосистемам с открытым ключом (несимметричным криптоалгоритмам).

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

В результате освоения дисциплины (модуля) формируются следующие компетенции:

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы компетенций	Результаты обучения
ОПК-4: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-4.1. Понимает особенности работы современных информационных технологий. ОПК-4.2. Анализирует принципы работы современных информационных технологий. ОПК-4.3. Использует современные информационные технологии для решения задач профессиональной деятельности	*Знать:* - о существующих средствах защиты информации и возможностях их использования в задачах создания и внедрения информационных систем; - принципы криптографических преобразований, типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа.
		Уметь: - проводить анализ степени защищённости информации; – - осуществлять повышение уровня защиты с учётом развития математического и программного обеспечения вычислительных систем.
		Владеть: - навыками применения современных алгоритмов для шифрования/ дешифрования секретной информации; - навыками решения практических задач профессиональной деятельности.

3. УКАЗАНИЕ МЕСТА ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина (модуль) «Защита информации» относится к обязательной части программы по направлению подготовки 01.03.02 Прикладная математика и информатика направленность (профиль) Управление данными и машинное обучение.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ С УКАЗАНИЕМ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ, ВЫДЕЛЕННЫХ НА КОНТАКТНУЮ РАБОТУ ОБУЧАЮЩИХСЯ С ПРЕПОДАВАТЕЛЕМ (ПО ВИДАМ УЧЕБНЫХ ЗАНЯТИЙ) И НА САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

Общая трудоемкость дисциплины (модуля) составляет 6 зачетные единицы или 216 часов (из расчета 1 ЗЕ = 36 часов).

Курс	Семестр	Трудоемкость в ЗЕ	Общая трудоемкость (час)	Контактная работа			Всего контактных часов	Из них в интерактивной форме	Кол-во часов на СРС		Кол-во часов на контроль	Форма контроля
				ЛК	ПР	ЛБ			Общее количество часов на СРС	Из них – на курсовую работу		
7	7	6	216	30	-	50	80	22	109		27	экзамен
Итого		6	216	30	-	50	80	22	109		27	экзамен

Интерактивная форма реализуется в виде кейс-заданий по тематикам дисциплины.

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

№ п/п	Наименование раздела, темы	Контактная работа			Всего контактных часов	Из них в интерактивной форме	Кол-во часов на СРС	Кол-во часов на контроль
		ЛК	ПР	ЛБ				
1.	Введение в информационную безопасность (ИБ). Уровни обеспечения ИБ.	6		10	16	4	20	
2.	Криптографическая защита данных.	6		10	16	4	20	
3.	Защита информации в компьютерных сетях.	6		10	16	4	20	
4.	Современные технологии защиты информации.	6		10	16	4	20	
5.	Законодательство РФ в области защиты данных и обеспечения ИБ.	6		10	16	6	19	
	Экзамен							27
	ИТОГО:	**30**		**50**	**80**	**22**	**99**	**27**

Содержание дисциплины (модуля)

Раздел 1. Введение в информационную безопасность (ИБ). Уровни обеспечения ИБ.

- Основные определения: информация, защищаемая информация, безопасность информации. Угрозы безопасности: угроза конфиденциальности, угроза целостности, угроза отказа в обслуживании. Защита информации. Направления защиты информации: правовая, техническая, криптографическая, физическая. Технологии информационной защиты.
- Стандарт «Критерии оценки безопасности информационных технологий» («Общие критерии» ISO/IEC 15408). Функциональные требования. Требования доверия.

Раздел 2. Криптографическая защита данных

- Основные определения: открытый текст, шифротекст, шифрование, дешифрование, криптография, криптоанализ, криптология.
- Классификация криптоалгоритмов: по типу преобразований, по типу использования ключей, по размеру преобразуемого блока.
- Одноалфавитные подстановки. Многоалфавитные подстановки. Перестановки по ключу
- Симметричные криптоалгоритмы (системы с секретным ключом). Скремблеры, как пример потокового шифра. Сеть Фейстеля и её применение в блочных шифрах. Шифры DES, ГОСТ 28147-89, Blowfish.
- Элементы теории чисел: сравнения и их свойства, функция Эйлера, малая теорема Ферма, алгоритм быстрого модулярного возведения в степень, алгоритм Евклида и его применение, дискретный логарифм (индекс числа), китайская теорема об остатках.
- Асимметричные криптоалгоритмы (системы с открытым ключом): протокол обмена ключами по алгоритму Диффи-Хеллмана, криптосистема RSA: шифрование, дешифрование, требования к ключам. Криптосистема Эль-Гамаля: шифрование, дешифрование. Электронная подпись: генерация и проверка подписи в криптосистеме Эль-Гамаля. Временная метка (Timestamp): создание и проверка временной метки.
- Способы разделения секрета между несколькими участниками
- Эллиптические кривые и их применение в криптографии
- Вычислительные проблемы криптологии: задача факторизации и способы её решения (метод силовой атаки. метод Полларда, метод Ферма), способы нахождения больших простых чисел (севдопростые числа, алгоритм Миллера-Рабина), Задача вычисления дискретного логарифма и способы её решения (метод Сильвера-Полига-Хеллмана согласования, метод Шенкса «больших и малых шагов»).

Раздел 3. Защита информации в компьютерных сетях.

- Технологии аутентификации. Основные определения: идентификация, аутентификация, авторизация, администрирование. Три группы методов аутентификации (“*I have*”, “*I know*”, “*I am*”). Биометрические методы аутентификации (статические и динамические). Простая аутентификация. Строгая аутентификация. Протоколы строгой аутентификации. Основные атаки на протоколы аутентификации.

- Технологии межсетевых экранов (МЭ). Функции межсетевых экранов. Фильтрация трафика. Выполнение функций посредничества. Дополнительные возможности МЭ.
- Технологии виртуальных защищенных каналов и сетей VPN. Концепция построения виртуальных защищенных сетей. VPN. VPN-решения для построения защищенных сете. Достоинства применения технологий VPN.
- Технологии обнаружения вторжений. Концепция адаптивного управления безопасностью. Технология анализа защищенности. Технологии обнаружения атак: методы анализа сетевой информации, классификация систем обнаружения атак IDS, компоненты и архитектура IDS, методы реагирования.
- Технологии защиты от вирусов. Компьютерные вирусы и проблемы антивирусной защиты: классификация компьютерных вирусов, жизненный цикл вирусов, основные каналы распространения вирусов и других вредоносных программ. Антивирусные программы и комплексы. Построение системы антивирусной защиты корпоративной сети.

Раздел 4. Современные технологии защиты информации.

- Противодействие сосредоточенным и распределенным DDOS атакам. Виды атак типа «отказ в обслуживании». Специфика атак.
- Построение многокомпонентных защищенных систем.
- Туннелирование и сокрытие информации при передаче по сетям общего пользования. Специальные межсетевые экраны.

Раздел 5. Законодательство РФ в области защиты данных и обеспечения информационной безопасности.

- Основные законные и подзаконные акты, статьи Конституции РФ, Кодексы и Регламенты.
- Законные определения основных понятий ИБ.
- Требования о защите информации в государственных структурах. Стандарт ГОСТ.
- Генерация и уничтожение информации.

6. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ, НЕОБХОДИМОГО ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Основная литература:

1. Внуков, А. А. Защита информации : учеб. пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 261 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01678-9. — Режим доступа : https://www.biblio-online.ru/book/zaschita-informacii-414082.
2. Лось, А. Б. Криптографические методы защиты информации : учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — М. : Издательство Юрайт, 2018. — 473 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-01530-0. — Режим доступа : https://www.biblio-online.ru/book/kriptograficheskie-metody-zaschity-informacii-413075.

Дополнительная литература:

3. Ляш, О. И. Сетевые технологии: теория и практика администрирования : учеб.-метод. пособие. Ч. 2 / Олег Иванович Ляш, Наталья Юрьевна Королева ; Федер. агентство по образованию, Мурм. гос. пед. ун-т. - Мурманск : МГПУ, 2010. - 201 с. : ил. - Библиогр.: с. 198-201 (46 назв.). - ISBN 978-5-4222-0044-3 : 58-09.
4. Информационные системы и технологии в экономике и управлении в 2 ч. Часть 2 : учебник для бакалавриата и специалитета / отв. ред. В. В. Трофимов. — 5-е изд., перераб. и доп. — М. : Издательство Юрайт, 2018. — 324 с. — (Серия : Бакалавр и специалист). — ISBN 978-5-534-09092-5. — Режим доступа : https://www.biblio-online.ru/book/informacionnye-sistemy-i-tehnologii-v-ekonomike-i-upravlenii-v-2-ch-chast-2-427127.

7.1 ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО И СВОБОДНО РАСПРОСТРАНЯЕМОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ:

7.1.1. Лицензионное программное обеспечение отечественного производства: нет

7.1.2. Лицензионное программное обеспечение зарубежного производства:

- Mathematica
- MathType
- MS Office
- Statistica

7.1.3. Свободно распространяемое программное обеспечение отечественного производства:

DJVuReader

7.1.4. Свободно распространяемое программное обеспечение зарубежного производства:

Adobe Reader

Mozilla FireFox

7.2 ЭЛЕКТРОННО-БИБЛИОТЕЧНЫЕ СИСТЕМЫ:

- ЭБС «Издательство Лань» [Электронный ресурс]: электронная библиотечная система / ООО «Издательство Лань». – Режим доступа: https://e.lanbook.com/;
- ЭБС «Электронная библиотечная система ЮРАЙТ» [Электронный ресурс]: электронная библиотечная система / ООО «Электронное издательство ЮРАЙТ». – Режим доступа: https://biblio-online.ru/;
- ЭБС «Университетская библиотека онлайн» [Электронный ресурс]: электронно-периодическое издание; программный комплекс для организации онлайн-доступа к лицензионным материалам / ООО «НексМедиа». – Режим доступа: https://biblioclub.ru/.

7.3 СОВРЕМЕННЫЕ ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ:

- Информационно-аналитическая система SCIENCE INDEX
- Электронная база данных Scopus
- Базы данных компании CLARIVATE ANALYTICS

7.4. ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ:

- Справочно-правовая информационная система Консультант Плюс http://www.consultant.ru/
- ООО «Современные медиа технологии в образовании и культуре» http://www.informio.ru/

8. ИНЫЕ СВЕДЕНИЯ И МАТЕРИАЛЫ НА УСМОТРЕНИЕ ВЕДУЩЕЙ КАФЕДРЫ.

Не предусмотрено.

9. ОБЕСПЕЧЕНИЕ ОБРАЗОВАНИЯ ДЛЯ ЛИЦ С ОВЗ.

Для обеспечения образования инвалидов и лиц с ограниченными возможностями здоровья реализация дисциплины может осуществляться в адаптированном виде, с учетом специфики освоения и дидактических требований, исходя из индивидуальных возможностей и по личному заявлению обучающегося.