Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Новгородский государственный университет имени Ярослава Мудрого»
Институт электронных и информационных систем
Кафедра прикладной математики и информатики

УТВЕРЖДАЮ
Директор ИЭИС
_____В.А. Шульцев
подпись
«_16_» ____06_____2023 г.
Число месяц

РАБОЧАЯ ПРОГРАММА
учебной дисциплины
Методы защиты информации

по направлению подготовки
01.03.02 Прикладная математика и информатика
направленность (профиль) Прикладная математика и информатика

СОГЛАСОВАНО
Начальник
Отдела обеспечения деятельности ИЭИС

_____И.Н. Гуркова .
(подпись)
«_16_» ____06____2023 г.
число месяц

Разработал
доцент кафедры ПМИ

_____ Т.В. Жгун

«12» июня _2023_ г.

Принято на заседании кафедры ПМИ

Протокол №10 от 14.06.2023 г.

Заведующий кафедрой ПМИ

_____ В.А. Едемский

«14 » _ июня _2023 г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 4783c4238c53ba4b6eaabef70b3cb643
Владелец: Шульцев Владимир Александрович
Действителен: с 24.01.2023 до 18.04.2024
НОВГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ ЯРОСЛАВА МУДРОГО

1 Цели и задачи освоения учебной дисциплины

Цель освоения учебной дисциплины: формирование компетентности студентов в области защиты информации, способствующей становлению их готовности к решению задач профессиональной деятельности; раскрытие сущности и значения информационной безопасности и защиты информации, определение методологических и технических основ различных аспектов защиты информации и связи между ними.

Понимание особенностей применения методов защиты информации является важнейшей частью компетентности специалиста в сфере профессиональной деятельности, кроме того, эффективные решения в профессиональной сфере в первую очередь основываются на анализе последствий адекватного или неадекватного применения методов защиты информации. Вследствие этого ставятся следующие **задачи:**

- определение базовых понятий информационной безопасности и защиты информации;
- определение угроз, каналов и способов несанкционированного доступа к информации;
- изучение основных методов и систем криптографической защиты информации; изучение основных типов политик безопасности и систем разграничения доступа;
- рассмотрение особенностей защиты информации в сетях;
- обзор нормативной базы в области защиты информации;
- формирование понимания студентами значимости знаний и умений в области защиты информации в процессе профессиональной деятельности;
- формирование системы знаний о методах защиты информации, позволяющей в будущем выстраивать на научной основе процессы профессиональной деятельности;
- подготовка студентов к профессиональной деятельности, связанной с выполнением проектов на основе современных информационных технологий.

2 Место учебной дисциплины в структуре ОПОП

Учебная дисциплина относится к обязательной части основной профессиональной образовательной программы направления подготовки01.03.02 Прикладная математика и информатика и направленности (профилю) Прикладная математика и информатика(далее – ОПОП).В качестве входных требований выступают сформированные ранее компетенции обучающихся, приобретенные ими в рамках следующих дисциплин: «Линейная алгебра и аналитическая геометрия», «Математический анализ», «Теория вероятностей и математическая статистика», «Информатика» и «Алгоритмические языки», «Дискретная математика».

Освоение учебной дисциплины может являться компетентностным ресурсом для прохождении производственной практики и для подготовки выпускной квалификационной работы.

3 Требования к результатам освоения учебной дисциплины

Перечень компетенций, которые формируются в процессе освоения учебной дисциплины:

Общепрофессиональные компетенции:

ОПК-4 Способен решать задачи профессиональной деятельности с использованием существующих информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

ОПК-5 Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения.

Результаты освоения учебной дисциплины представлены в таблице 1.

Таблица 1–Результаты освоения учебной дисциплины

Код и наименование компетенции	*Результаты освоения учебной дисциплины (индикаторы достижения компетенций)*		
ОПК-4 Способен решать задачи профессиональной деятельности с использованием существующих информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-4.1 Знать современные образовательные и информационные технологии, информационные системы и ресурсы, необходимое специализированное программное обеспечения для решения профессиональных задач; причины нарушения компьютерной безопасности; методы сбора и обработки и хранения информации	ОПК-4.2 Уметь использовать научные и методические ресурсы сети Интернет для разработки программного обеспечения и с учетом требований информационной безопасности;использовать информационные сервисы глобальных телекоммуникаций, базы данных, web-ресурсы, системное и программное обеспечение	ОПК-4.3Владеть навыками работы в информационных современных системах автоматического поиска для получения необходимой информации;базовыми знаниями по защите информации на рабочем месте, в корпоративных сетях при входе в глобальные сети;навыками системного и объектно-ориентированного программирования для решения стандартных прикладных задач в профессиональной деятельности
ОПК-5 Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения	ОПК-5.1 Знать -методы алгоритмизации, алгоритмические языки и технологии программирования, пригодные для практического применения в области информационных систем и технологий; - основные языки программирования и работы с базами данных, операционные системы и оболочки, современные программные среды разработки информационных систем и технологий;	ОПК-5.2 Уметь - применять методы алгоритмизации, алгоритмические языки и технологии программирования, пригодные для практического применения в области информационных систем и технологий; - применять языки программирования и работы с базами данных, современные программные среды разработки информационных систем и технологий для автоматизации бизнес-процессов, решения прикладных задач различных	ОПК-5.3Владеть - методами алгоритмизации, алгоритмическими языками и технологиями программирования, пригодными для практического применения в области информационных систем и технологий; - владеть навыками программирования, отладки и тестирования прототипов

		классов, ведения баз данных программно-технических комплексов задач и информационных хранилищ.	

4 Структура и содержание учебной дисциплины

4.1 Трудоемкость учебной дисциплины

4.1.1 Трудоемкость учебной дисциплины для очной формы обучения представлена в таблице 2.

Таблица 2 –Трудоемкость учебной дисциплины для очной формы обучения

Части учебной дисциплины	*Всего*	*Распределение по семестрам*
		8 семестр
1. Трудоемкость учебной дисциплины в зачетных единицах (ЗЕТ)	6	6
2. Контактная аудиторная работа в академических часах (АЧ)	70	70
3. Курсовая работа/курсовой проект (АЧ) *(при наличии)*	0	0
4. Внеаудиторная СРС в академических часах (АЧ)	146	146
5. Промежуточная аттестация (*зачет; дифференцированный зачет; экзамен*) (АЧ)	*Экзамен*	*Экзамен*

4.1.2 Трудоемкость учебной дисциплины для заочной/очно-заочной формы обучения: не предусмотрено учебным планом.

4.2 Содержание учебной дисциплины

1. Введение. Роль информации в современном обществе. Проблемы информации вообще и управления как информационный процесс. Основные понятия и определения, относящиеся к информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности; классификация атак; модели сетевой безопасности и безопасности информационной системы.

2. Понятие стеганографии. Методы и средства встраивания скрытой служебной информации для управления правами доступа к информационным ресурсам. Задача встраивания скрытой служебной информации (цифровых водяных знаков) в аудио и видеосигналы. Основные методы и алгоритмы встраивания и обнаружения водяных знаков. Стегоанализ.

3. Традиционное шифрование: классические методы. Основные понятия и определения. Подстановочные и перестановочные шифры. Шифры Цезаря, Виженера,

Вернама. Дисковые шифраторы. Исследования Шеннона в области криптографии. Нераскрываемость шифра Вернама. Различные способы создания псевдослучайных чисел

4. Алгоритмы симметричного шифрования. Основные понятия, относящиеся к алгоритмам симметричного шифрования: ключ шифрования, plaintext, ciphertext. Определение стойкости алгоритма, типы операций, используемые в алгоритмах симметричного шифрования. Сеть Фейштеля. Основные понятия криптоанализа, линейный и дифференциальный криптоанализ. Описание стандартов шифрования алгоритмов DES и тройного DES, ГОСТ 28147. Режимы их выполнения. Стандарт шифрования AES.

5. Асимметричные системы шифрования (системы с открытым ключом). Математические основы современной криптографии. Понятия однонаправленной функции и однонаправленной функции с лазейкой. Функции дискретного логарифмирования и основанные на ней алгоритмы: схема Диффи-Хеллмана, схема Эль-Гамаля. Схема RSA: алгоритм шифрования, его обратимость, вопросы стойкости

6. Хэш-функции и аутентификация сообщений. Основные понятия, относящиеся к обеспечению целостности сообщений с помощью MAC и хэш-функций; представлены простые хэш-функции и сильная хэш-функция MD5. Сильные хэш-функции SHA-1, SHA-2 и ГОСТ 3411. Основные понятия, относящиеся к обеспечению целостности сообщений и вычислению MAC с помощью алгоритмов симметричного шифрования, хэш-функций и алгоритма HMAC.

7. Цифровая подпись. Основные требования к цифровым подписям, прямая и арбитражная цифровая подпись, стандарты цифровой подписи ГОСТ 3410 и DSS.

8. Криптография с использованием эллиптических кривых. Математические понятия, связанные с эллиптическими кривыми, в частности задача дискретного логарифмирования на эллиптической кривой. Аналог алгоритма Диффи-Хеллмана на эллиптических кривых, алгоритма цифровой подписи на эллиптических кривых и алгоритма шифрования с открытым ключом получателя на эллиптических кривых.

9. Безопасность современных сетевых технологий. Способы несанкционированного доступа к информации в компьютерных сетях. Классификация способов несанкционированного доступа и жизненный цикл атак.Способы противодействия несанкционированному межсетевому доступу. Функции межсетевого экранирования. Обзор протоколов. Безопасность в открытых сетях**.** Инфраструктура на основе криптографии с открытыми ключами (ИОК). Цифровые сертификаты. Управление цифровыми сертификатами. Управление ключами.

4.3 Трудоемкость разделов учебной дисциплины и контактной работы

Таблица 3 – Трудоемкость разделов учебной дисциплины

№	Наименование разделов (тем) учебной дисциплины, УЭМ, наличие КП/КР	Контактная работа (час)						Внеауд. СРС (час)	Формы текущего контроля
		Аудиторная			В т.ч. ауд. СРС	КР	ЭКЗ		
		ЛЕК	ПЗ	ЛР					
8 семестр									
1	Введение. Стеганография.	4			2			16	
2	Традиционное шифрование	6	4	6	2			30	Индивидуальное практическое задание Лабораторная работа
3	Алгоритмы симметричного шифрования	8	4	8	2			30	Лабораторная работа Лабораторная работа
4	Математические основы криптографии. Системы с открытым ключом	4	4	8	2			30	Лабораторная работа
5	Хэш-функции и аутентификация сообщений. Цифровая подпись	4	2	6	2			20	Лабораторная работа Индивидуальное практическое задание
6	Криптография с использованием эллиптических кривых. Безопасность современных сетевых технологий	2			2			20	
	Промежуточная аттестация						*36*		*экзамен*
	ИТОГО за 8 семестр	**28**	**14**	**28**	**12**		**36**	**146**	

4.4 Лабораторные работы и курсовые работы/курсовые проекты

4.4.1 Перечень тем лабораторных работ:
Традиционное шифрование
Стандарты симметричного шифрования. VS-AES
Математические основы криптографии
Системы с открытым ключом
Аутентификация сообщений. Цифровая подпись

4.4.2 Примерные темы курсовых работ/курсовых проектов:
Курсовые работы/курсовые проекты не предусмотрены учебным планом

5 Методические рекомендации по организации освоения учебной дисциплины

Таблица 4 –Методические рекомендации по организации лекций

№	*Темы лекционных занятий (форма проведения)*	*Трудоем-кость в АЧ*
1	Введение. Стеганография (вводная лекция с элементами проблемной лекции)	4
2	Традиционное шифрование(лекция-презентация)	6
3.	Алгоритмы симметричного шифрования (проблемная лекция, рефлексия полученных образовательных результатов)	6
4	Математические основы криптографии. Системы с открытым ключом (лекция-презентация)	8
5	Хэш-функции и аутентификация сообщений. Цифровая подпись (проблемная лекция, рефлексия полученных образовательных результатов)	2
6	Криптография с использованием эллиптических кривых. Безопасность современных сетевых технологий (лекция-презентация)	2
	ИТОГО	28

Таблица 5–Методические рекомендации по организации практических занятий

№	*Темы практических занятий (форма проведения)*	*Трудоем-кость в АЧ*
1.	Традиционное шифрование	4
2.	Алгоритмы симметричного шифрования	4
3.	Математические основы криптографии. Системы с открытым ключом	4
4.	Хэш-функции и аутентификация сообщений. Цифровая подпись	2
	ИТОГО	14

Задания для практических работ и описание методики выполнения содержатся в учебном пособии:
Методы защиты информации : метод.указания по практическим занятиям для направления 01.03.02 "Прикладная математика и информатика" / сост. Т. В. Жгун. – Великий Новгород. ИздательствоНовГУ . 2017.– 62 с. – ББК 32.973.2-018+22.161я73– Текст электронный – Электронно-библиотечная система БиблиоТех. [сайт]. –URL: https://novsu.bibliotech.ru/Reader/Book/-2568 (дата обращения 10.11.2022)

Самостоятельная работа студентов: в учебном процессе выделяют два вида самостоятельной работы – аудиторная и внеаудиторная. Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию. Внеаудиторная самостоятельная работа выполняется студентом по заданию преподавателя, но без его участия. Самостоятельная работа включает изучение теоретического материала, подготовку к тестированию, выполнение определенных заданий расчётно-практической работы и индивидуального практического задания.

Практические занятия проводятся в компьютерном классе с современными ПК с подключением к сети «Интернет» и установленным лицензионным программным обеспечением. Лекционные занятия проводятся в аудитории, оборудованной мультимедийной проекционной системой с интерактивной доской или экраном.

Лабораторные работы имеют своей целью научить студентов применять методы приближенных вычислений для решения конкретных задач с компьютера с помощью пакетов прикладных программ и/или языков программирования высокого уровня и оценивать погрешность получаемого результата, углубить практические навыки работы с компьютерной техникой, овладеть методикой экспериментальных исследований в области вычислительной математики и обработки полученных результатов.

При проведении лабораторного практикума студенты самостоятельно выполняют лабораторные работы, получая необходимые консультации у преподавателя. Отчет оформляется в соответствии с СТО 1.701-2010. Текстовые документы. Общие требования к построению и оформлению. Перечень ЛР указан в разделе 4.4 настоящей рабочей программы.

Задания на лабораторные работы содержатся в учебном пособии:
Методы защиты информации : метод.указания к выполнению лабораторных работ для направления 01.03.02 "Прикладная математика и информатика" / сост. Т. В. Жгун. – Великий Новгород. ИздательствоНовГУ . 2017.– 62 с. – ББК 32.973.2-018+22.161я73– Текст электронный – Электронно-библиотечная система БиблиоТех. [сайт]. –URL: https://novsu.bibliotech.ru/Reader/Book/-2568 (дата обращения 10.11.2022)

6 Фонд оценочных средств учебной дисциплины

Фонд оценочных средств представлен в Приложении А.

7 Условия освоения учебной дисциплины

7.1 Учебно-методическое обеспечение

Учебно-методического обеспечение учебной дисциплины представлено в Приложении Б.

7.2 Материально-техническое обеспечение учебной дисциплины

Таблица 6 – Материально-техническое обеспечение учебной дисциплины

№	*Требование к материально-техническому обеспечению*	*Наличие материально-технического оборудования и программного обеспечения*
1	Учебные аудитории для проведения учебных занятий	Учебная мебель: столы, стулья, доска
		Компьютерный класс, проектор, интерактивная доска
2	Мультимедийное оборудование	Проектор, компьютер, экран, интерактивная доска

Программное обеспечение

Наименование программного продукта	**Обоснование для использования (лицензия, договор, счёт, акт или иное)**	**Дата выдачи**
Academic VMware Workstation 16 Pro for Linux and Windows, ESD	Договор №211/ЕП(У)20-ВБ, 25140763	03.11.2020
Acronis Защита Данных для рабочей станции, Acronis Защита Данных. Расширенная для физического сервера	Договор №210/ЕП (У)20-ВБ, Ах000369127	03.11.2020
Антиплагиат. Вуз. *	Договор №3341/12/ЕП(У)21-ВБ	29.01.2021
«Kaspersky Endpoint Security для бизнеса - Стандартный Russian Education Renewal. 250-499 Node I year License» /1 год *	Договор №158/ЕП(У)22-ВБ	21.09.2022
Astra Linux Special Edition*	195200041-alse-1.7-client-base_orel-x86_64-0-14211	09.12.2022
* отечественное производство		

Свободно распространяемое программное обеспечение

Наименование ПО	*Лицензия*	*Официальный сайт*	*Описание*
Teams	Freeware	https://www.microsoft.com/ru-ru/microsoft-teams/free?market=ru	
Skype	Freeware	https://www.skype.com/ru/get-skype/	
Zoom	Freeware	https://zoom.us/downloadcenter	
MS Office 365	Безвозмездно передаваемое ВУЗам		
Microsoft Visual Studio 2010	Freeware	http://www.microsoft.com/visualstudio/ru-ru	Среда программирования
Eclipse IDE	Eclipse Public License	http://eclipse.org/	Интегрированная среда разработки
FreeMat	GPL	https://freemat.sourcefor ge.net/	среда для прототипирования и обработки данных (аналог matlab с открытым исходным кодом)
Google Chrome	Freeware	https://google.com/	Браузер
IDLE	PSFL	https://python.org/idle	Интегрированная среда разработки
Java Development Kit	Sun License	https://www.oracle.com/java/technologies/downloads/	комплект разработчика приложений на java
Lazarus	GNU LGPL	https://www.lazarus-ide.org/	Интегрированная среда разработки
Maxima	GNU GPL	https://maxima.sourceforge.io/ru/index.html	система компьютерной алгебры
Mozilla Firefox	MPL, GNU GPL	http://mozilla.org/	Браузер
NodeJS	MIT	https://nodejs.org/en/	Среда выполнения JavaScript
Python	Python Software Foundation License	https://www.python.org	язык программирования Python
R	GNU GPL v2	http://www.r-project.org/	язык программирования R
R for Windows	Freeware	GNU General Public License	https://cran.r-project.org/bin/windows/base/
WinDjView	GNU GPL	http://windjview.sf.net/ru/	Просмотрщик DjVu
7zip	GNU LGPL	http://7-zip.org/	Архиватор
Adobe Acrobat	Freeware	http://adobe.com	Чтение PDF
AnyLogic PLE Freeware	Freeware	https://www.anylogic.ru/s/download-free-simulation-software-for-education/	имитационное моделирование
AnyLogic PLE	Freeware	https://www.anylogic.ru/s/download-free-simulation-software-for-education/	имитационное моделирование

Приложение А
(обязательное)

Фонд оценочных средств
учебной дисциплины «Методы защиты информации»

1 Структура фонда оценочных средств

Фонд оценочных средств состоит их двух частей:

а) открытая часть – общая информация об оценочных средствах (название оценочных средств, проверяемые компетенции, баллы, количество вариантов заданий, методические рекомендации для применения оценочных средств и пр.), которая представлена в данном документе, а также те вопросы и задания, которые могут быть доступны для обучающегося;

б) закрытая часть – фонд вопросов и заданий, которая не может быть заранее доступна для обучающихся (вопросы тестов, вопросы к проверочным работам и пр.) и которая хранится в закрытом виде (банк вопросов).

2 Перечень оценочных средств текущего контроля и форм промежуточной аттестации

Таблица А.1 –Перечень оценочных средств

№	*Оценочные средства для текущего контроля*	*Разделы (темы) учебной дисциплины*	*Баллы*	*Проверяемые компетенции*
1	Индивидуальное практическое задание	Традиционное шифрование	2*25	ОПК-4 ОПК-5
2	Индивидуальное практическое задание	Системы с открытым ключом. Аутентификация сообщений. Цифровая подпись	2*25	ОПК-4
3	Лабораторная работа	Традиционное шифрование	30	ОПК-4 ОПК-5
4	Лабораторная работа	Стандарты симметричного шифрования. VS-AES	30	ОПК-4
5	Лабораторная работа	Математические основы криптографии	30	ОПК-4
6	Лабораторная работа	Системы с открытым ключом	30	ОПК-4
7	Лабораторная работа	Аутентификация сообщений. Цифровая подпись	30	ОПК-4
Промежуточная аттестация				
	Экзамен		**50**	ОПК-4
	ИТОГО		**300**	

3 Рекомендации к использованию оценочных средств

1) Лабораторные работы

Критерии оценки	*Количество вариантов заданий*	*Количество заданий в одном варианте*
Соответствие выполненной работы описанию – 6 баллов	15	согласно описанию работы
Корректность описания задания – 6 баллов		
Полнота выполнения работы – 6 баллов		
Полнота информации в отчёте и логичность её изложения – 6 баллов		
Оригинальность и креативность выполнения задания – 6 баллов		

Задания на лабораторные работы содержатся в учебном пособии:

Жгун Т.В. Методы защиты информации. Методические указания по выполнению лабораторных работ. [Электронный ресурс]: методические указания. – Великий Новгород, 2013. – 40 с. – Режим доступа: https://novsu.bibliotech.ru/Catalog/Index

Список возможных вопросов для собеседования по лабораторным работам

Собеседование по 1й лабораторной работе

1. Какой шифр называется шифром подстановки?
2. Какой шифр называется шифром перестановки?
3. Какой шифр называется поворотной решеткой?
4. Какой шифр называется шифром вертикальной перестановки?
5. К какому классу шифров относится шифр Цезаря?
6. Что такое гамма и гаммирование?
7. В чем заключается шифрование по Вижинеру?

Собеседование по 2й лабораторной работе

1. Что называется ключом шифрования.
2. Какие шифры называются шифрами на открытом ключе и какие – шифрами на секретном ключе?
3. Ответ : в шифрах на секретном ключе один и тот же ключ используется как для шифрования, так и для дешифрования данных. В шифрах на открытом ключе при шифровании и дешифровании используются разные ключи: открытый и общеизвестный – при шифровании, закрытый, секретный – при дешифровании.
4. Чем отличается поточное шифрование от блочного?
5. Чему равна длина секретного ключа алгоритма DES?
6. Чему может быть равна длина секретного ключа алгоритма Rijndael?
7. Какая архитектура лежит в основе алгоритма DES?
8. Какой параметр определяет криптостойкость современного алгоритма?
9. Что такое ECB, CBC

Собеседование по 3й лабораторной работе

1. Какая процедура является более производительной – асимметричное шифрование/дешифрование или симметричное шифрование/дешифрование?

2. К какому типу криптоалгоритма (с точки зрения его устойчивости к взлому) и почему относится алгоритм RSA?
3. Какая трудноразрешимая математическая задача лежит в основе стойкости алгоритма RSA?
4. Какая трудноразрешимая математическая задача лежит в основе стойкости алгоритма Эль Гамаль?
5. В чем заключается проблема дискретного логарифма?
6. В чем заключаются проблемы разложения больших чисел на простые множители и вычисления корней алгебраических уравнений?

Собеседование по 4й лабораторной работе

1. Что называется ключом шифрования.
2. Какие шифры называются шифрами на открытом ключе и какие – шифрами на секретном ключе?
3. Чем отличается поточное шифрование от блочного?
4. Чему равна длина секретного ключа алгоритма DES?
5. Чему может быть равна длина секретного ключа алгоритма Rijndael? Какая архитектура лежит в основе алгоритма DES?
6. Какой параметр определяет криптостойкость современного алгоритма?
7. Что такое ECB, CBC

Собеседование по 5й лабораторной работе

1. Что такое хэш-функция? Зачем она нужна?
2. Что называется электронной цифровой подписью?
3. Для чего используется ЭЦП?
4. ЭЦП используется для аутентификации отправителя сообщений и того, чтобы сделать сообщение неотвергаемым?
5. Что такое дайджест-сообщение?
6. Что такое вычислительно необратимая функция?

2) Индивидуальное практическое задание

Критерии оценки	*Количество вариантов заданий*	*Количество заданий в одном варианте*
Соответствие выполненной работы описанию – 5 баллов	15	согласно описанию работы
Корректность описания задания – 5баллов		
Полнота выполнения работы – 5 баллов		
Полнота информации в отчёте и логичность её изложения – 5баллов		
Оригинальность и креативность выполнения задания – 5баллов		

Индивидуальное практическое задание 1

Вариант выбирается по списку группы

Задание 1

Зашифровать сообщение с помощью маршрутной транспозиции с помощью двойной перестановки строк и столбцов, определяемой паролем. Выбор открытого текста осуществляется по табл.1 в соответствии с номером студента в списке группы. Пароль выбирается из этой же таблице. Размер таблицы для шифрования 5×6. Первые 5 различных символов пароля служат для перестановки столбцов, 6 следующих символов служат для перестановки строк.

P= N; K= 26-N

В пароле используются только неповторяющиеся символы.

Задание 2

С помощью «квадрата Полибия» зашифровать сообщение. Выбор открытого текста осуществляется по табл.1 в соответствии с номером студента в списке группы. Пароль выбирается из этой же таблице. Размер таблицы для шифрования 5×6.

P= N; K= 26-N

В пароле используются только неповторяющиеся символы.

Таблица 1 – Выбор открытого текста для шифрования

№	Открытый текст
1	Повадится овца не хуже козы
2	Не робей, воробей, держись орлом.
3	Не разводи усок на чужой кусок
4	Сурьма косых глаз не исправит.
5	сухой по мокрому не тужит.
6	Повадится овца не хуже козы.
7	Повадки волчьи, а душа заячья
8	По хозяину и собаке честь.
9	Поздно щуке на сковороде вспоминать о воде.
10	Поле глазасто, а лес ушаст.
11	Порозно думать вместе не жить
12	Посуленному только дурак рад.
13	Промеж худых и хорошему плохо..
14	Проживет Фаддей и без затей
15	Пуст мешок стоять не будет.
16	Под каждой крышей свои мыши
17	Пустой колос голову кверху носит.
18	Порозно думать вместе не жить
19	Родной куст и зайцу дорог.
20	Спесь росту не прибавит.
21	Не пойман-не вор, не уличена - не гулёна.
22	Не разводи усок на чужой кусок
23	сухой по мокрому не тужит
24	Не робей, воробей, держись орлом.
25	Повадки волчьи, а душа заячья

Индивидуальное практическое задание 2

Задание 1

С помощью шифра Вижинера зашифровать сообщение. Выбор открытого текста осуществляется по табл.1 в соответствии с номером студента в списке группы. Пароль выбирается из этой же таблице.

$P = N$
$K = 26\text{-}N$

Задание 2

С помощью шифра Пфайфера зашифровать сообщение. Выбор открытого текста осуществляется по табл.1 в соответствии с номером студента в списке группы. Пароль выбирается из этой же таблице. Размер таблицы для шифрования 5×6.

$P = NK = 26\text{-}N$

В пароле используются только неповторяющиеся символы. Длина пароля 7 символов. Разделителем служит символ «х».

Таблица 2 – Таблица Вижинера

а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а
в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б
г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в
д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г
е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д
ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е
з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж
и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з
й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и
к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й
л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к
м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л
н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м
о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н
п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о
р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п
с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р
т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с
у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т
ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у
х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф
ц	ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х
ч	ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц
ш	щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч
щ	ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
ъ	ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
ы	ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ
ь	э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы
э	ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь
ю	я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э
я	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю

Индивидуальное практическое задание 3.

Вариант выбирается по списку группы.

Задание 1

Вычислить 2 итерации, используя сеть Файстеля. Размер блока - 4 бита. С качестве нелинейной функции А использовать инверсию элементов блока. Открытый текст и ключ выбираем в таблице 3. в соответствии с номером студента в списке группы.

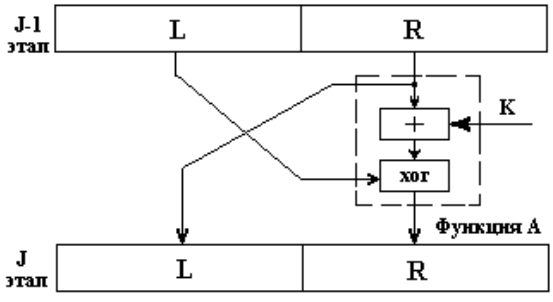

Таблица 3 – Открытый текст и ключ

№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Открытый текст	5	8	7	4	11	13	6	10	14	6	2	15	5	8	7	4	11	13	6	10	14	6	2	15	4
Ключ	4	11	13	6	10	14	6	2	15	5	8	7	4	11	13	6	10	14	6	2	15	4	15	5	8

Задание 2

Вычислить 1 итерацию алгоритма DES. Размер блока - 64 бита. Открытый текст – строка из нулей. Ключ выбираем в таблице 3 в соответствии с номером студента в списке группы.

Таблица 4 – Ключ

№	1	2	3	4	5	6	7	8	9	10	11	12	13
Ключ	2^16+2	2^16+2^15	2^16	2^15+2	1	2^15	2^16+2	2^16+2^15	2^16	2^15+2	1	2^15	2^16+2
№	14	15	16	17	18	19	20	21	22	23	24	25	
Ключ	2^16+2^15	2^16	2^15+2	1	2^15	2^16+2	2^16+2^15	2^16	2^15+2	1	2^15	2^16+2	

Таблица 5 – Вычисление ключей в алгоритме DES.
(а) перестановка со сжатием

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

(в) таблица сдвигов влево

Номер раунда	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Число сдвигов	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Таблица 6 - Определение S-матриц алгоритма DES.

S1	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	4	1	12	8	13	6	2	11	15	12	9	7	3	10	5	0
	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S3	10	0	99	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Таблица 7 (а) начальная перестановка IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

(б) перестановка, обратная начальной IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	53	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

(в) перестановка с расширением E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	27
28	29	30	31	32	1

(г) перестановка P

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Индивидуальное практическое задание 4
Задание 1

Вычислить 1 итерацию алгоритма ГОСТ. Размер блока - 64 бита. Открытый текст – строка из нулей. Ключ выбираем в таблице 3 в соответствии с номером студента в списке группы.

Таблица 8 – Выбор ключа

№	1	2	3	4	5	6	7	8	9	10	11	12	13
Ключ	2^16+2	2^16+2^15	2^16	2^15+2	1	2^15	2^16+2	2^16+2^15	2^16	2^15+2	1	2^15	2^16+2
№	14	15	16	17	18	19	20	21	22	23	24	25	
Ключ	2^16+2^15	2^16	2^15+2	1	2^15	2^16+2	2^16+2^15	2^16	2^15+2	1	2^15	2^16+2	

Таблица 9 – S-box алгоритма ГОСТ.

Номер S-блока	**Значение**
1	4 10 9 2 13 8 0 14 6 11 1 12 7 15 5 3
2	14 11 4 12 6 13 15 10 2 3 8 1 0 7 5 9
3	5 8 1 13 10 3 4 2 14 15 12 7 6 0 9 11
4	7 13 10 1 0 8 9 15 14 4 6 12 11 2 5 3
5	6 12 7 1 5 15 13 8 4 10 9 14 0 3 11 2
6	4 11 10 0 7 2 1 13 3 6 8 5 9 12 15 14
7	13 11 4 1 3 15 5 9 0 10 14 7 6 8 2 12
8	1 15 13 0 5 7 10 4 9 2 3 14 6 11 8 12

Задание 2

Вычислить дискретный логарифм элемента поля. Выбор поля и элемента осуществляется по табл.2 в соответствии с номером студента в списке группы. Пароль выбирается из этой же таблице.

Таблица 10 – Выбор конечного поля и элемента

№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Поле GF	2^4	3^3	5^2	47	2^4	3^3	5^2	47	2^4	3^3	5^2	47	2^4	3^3	5^2	47	2^4	3^3	5^2	47	2^4	3^3	5^2	47	2^4
Элемент	54	47	32	64	74	54	47	32	64	74	54	47	32	64	74	54	47	32	64	74	54	47	32	64	74

3) Экзамен

Критерии оценки	*Количество вариантов заданий*	*Количество вопросов*
45-50 – Демонстрирует всестороннее и глубокое знание материала модуля	25	3
35-44 – Допускает неточности при демонстрации знаний		
25-34 – Испытывает трудности при демонстрации знаний		

Пример экзаменационного билета:

Новгородский государственный университет имени Ярослава Мудрого
Кафедра прикладной математики и информатики
ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № X
Учебная дисциплина «**Методы защиты информации**». Семестр 8.
Для направления подготовки 01.03.02Прикладная математика и информатика

1. . Решить в $GF\left(2^3\right)$ систему $\begin{cases} 2x + y = 3 \\ x + 2y = 2 \end{cases}$

2. Выработать секретный ключ по алгоритму Диффи-Хеллмана с абонентом В, который задумал секретное число 3. Открытый ключ (17, q), где q – примитивный элемент поля GF(17).

3. Блочные криптосистемы с секретным ключом. Режимы работы. ГОСТ 28147-89 в режиме простой замены.

Принято на заседании кафедры «____»_____ 20___ г. Протокол № _____

Зав. кафедрой ПМИ

Вопросы к экзамену по учебной дисциплине
«Методы защиты информации»

1 Основные понятия и определения информационной безопасности: атаки, уязвимости, политика безопасности, механизмы и сервисы безопасности. Классификация атак. Модели сетевой безопасности и безопасности информационной системы.

2 Классическая задача криптографии. Угрозы со стороны злоумышленника и участников процесса информационного взаимодействия.

3 Шифры замены и перестановки. Моно- и многоалфавитные подстановки Шифры Цезаря, Виженера, Вернама. Методы дешифрования.

4 Классификация методов дешифрования. Модель предполагаемого противника. Правила Керкхоффа.

5 Совершенная секретность по Шеннону. Примеры совершенно секретных систем. Шифр Вернама. Понятие об управлении ключами.

6 Блочные криптосистемы с секретным ключом. Алгоритм DES. Описание DES. Основные этапы алгоритма.

7 Схема алгоритма DES. Раунд алгоритма. Преобразование ключа.

8 Алгоритм DES. Подстановка с помощью S-блоков. Расшифрование в DES.

9 Блочные криптосистемы с секретным ключом. Режимы работы. ГОСТ 28147-89 в режиме простой замены.

10 Поточные криптосистемы с секретным ключом. Синхронные и самосинхронизирующиеся поточные криптосистемы. Примеры. ГОСТ 28147-89 в режимах гаммирования.

11 Стандарт криптографической защиты 21 века(AES). Алгоритмы Rijndael и RC6. Математические понятия, лежащие в основе алгоритма Rijndael. Структура шифра.

12 Теория сложности вычислений. Классификация алгоритмов.

13 Алгоритм RSA. Математическая модель алгоритма. Стойкость алгоритма.

14 Криптосистема Эль-Гамаля.

15 Электронная подпись. Варианты электронной подписи на основе алгоритмов RSA и Эль-Гамаля.

16 Хэш-функции и их применение. Хеш-функция MD2.

17 Однонаправленные (односторонние) функции с секретом и их применение.

18 Обобщенная модель электронной цифровой подписи. Схема Диффи-Хеллмана, схема Эль-Гамаля.

19 Цифровая подпись на основе алгоритма RSA.

20 Стандарт цифровой подписи DSS. Генерация цифровой подписи. Проверка цифровой подписи.

21 Основные протоколы аутентификации и обмена ключей с использованием третьей доверенной стороны. Протоколы аутентификации с использованием nonce и временны́х меток.

22Криптографические протоколы. Понятие криптографического протокола и обоснование необходимости их использования. Протокол обмена сеансовыми ключами. Вскрытие "человек-в-середине". Протокол "держась за руки".

23 Сертификация ключей с помощью цифровых подписей. Разделение секрета. Метки времени. Пример протокола защиты базы данных.

24 Основы криптоанализа. Обзор возможных вариантов криптоанализа. Метод вскрытия «встреча посередине». Вскрытие со словарем. Вскрытие системы Вижинера, использующей простой XOR. Метод бесключевого чтения RSA. Атака на подпись RSA по выбранномушифротексту. Вскрытие хэш-функций с использованием парадокса дня рождения.

25 Криптосистемы на эллиптических кривых.

Приложение Б
(обязательное)

Карта учебно-методического обеспечения
учебной дисциплины «Методы защиты информации»

Таблица 1 – Основная литература*

Библиографическое описание издания (автор, наименование, вид, место и год издания, кол. стр.)	Кол. экз. в библ. НовГУ	Наличие в ЭБС
Печатные источники		
Мельников В. П. Защита информации : учебник : для бакалавров / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под ред. В. П. Мельникова. - Москва : Академия, 2014. - 295, [2] с. : ил. - (Высшее образование, Информационная безопасность) (Бакалавриат). - Библиогр.: с. 291-293. - ISBN 978-5-4468-0332-3 : (в пер.) : 512.60. - 701.25, 1500 экз.	4	
Лапонина О.Р. Основы сетевой безопасности:криптографические алгоритмы и протоколы взаимодействия : курс лекций : учебное пособие / Под ред.В .А.Сухомлина. - Москва : Интернет-Университет Информ. Технологий, 2005. - 604,[1]с. - Библиогр.: с. 604-605. - Слов.: с. 599-603. - ISBN 5-9556-0020-5 : (в пер.) : 498.00. Электронная версия курса https://www.studmed.ru/laponina-o-r-osnovy-setevoy-bezopasnosti-kriptograficheskie-algoritmy-i-protokoly-vzaimodeystviya_4591d74fac3.html	2	studmed.ru – общедоступный ресурс, осуществляет свою деятельность с соблюдением действующего законодательства РФ. 1
Электронные ресурсы		
Конспект лекций по курсу "Методы защиты информациии" для специальности 01.03.02 "Прикладная математика и информатика" / сост. Т. В. Жгун. – Великий Новгород. ИздательствоНовГУ . 2017.– 165 с. – ББК 32.973.2-018+22.161я73– Текст электронный – Электронно-библиотечная система БиблиоТех. [сайт]. –URL: https://novsu.bibliotech.ru/Reader/Book/-2574 (дата обращения 10.05.2023)		bibliotech
Методы защиты информации : метод.указания по практическим занятиям для направления 01.03.02 "Прикладная математика и информатика" / сост. Т. В. Жгун. – Великий Новгород. ИздательствоНовГУ . 2017.– 62 с. – ББК 32.973.2-018+22.161я73– Текст электронный – Электронно-библиотечная система БиблиоТех. [сайт]. –URL: https://novsu.bibliotech.ru/Reader/Book/-2568 (дата обращения 10.05.2023)		bibliotech
Методы защиты информации : метод.указания к выполнению лабораторных работ для направления 01.03.02 "Прикладная математика и информатика" / сост. Т. В. Жгун. – Великий Новгород. ИздательствоНовГУ . 2017.– 62 с. – ББК 32.973.2-018+22.161я73– Текст электронный – Электронно-библиотечная система БиблиоТех. [сайт]. –URL: https://novsu.bibliotech.ru/Reader/Book/-2568 (дата обращения 10.05.2023)		bibliotech

**См. требования п. 4.3.3 ФГОС 3++ (как правило, при использовании в образовательном процессе печатных изданий библиотечный фонд должен быть укомплектован печатными изданиями из расчета не менее 0,25 экземпляра на каждого из изданий, указанных в рабочих программах дисциплин (модулей), на одного обучающегося из числа лиц, одновременно осваивающих соответствующую дисциплину (модуль)).*

Таблица.2 – Дополнительная литература

Библиографическое описание издания (автор, наименование, вид, место и год издания, кол.стр.)	Кол.экз. в библ. НовГУ	Наличие в ЭБС
Печатные источники		
Рябко Б.Я. Криптографические методы защиты информации : учебное пособие для вузов. - Москва : Горячая линия-Телеком, 2005. - 229с. - Библиогр.: с. 218-221. - Указ.: с. 222-226. - ISBN 5-93517-265-8 : (в пер.) : 229.00.	3	
– **Рябко Б.Я.** Основы современной криптографии для специалистов в информационных технологиях / РАН, Ин-т вычисл.технологий; Сиб.гос.ун-т телекоммуникаций и информатики. - Москва : Научный мир, 2004. - 172с. - Библиогр.: с. 170-172. - ISBN 5-89176-233-1 : (в пер.) : 70.00. - 178.00	4	
Молдовян Н.А. Практикум по криптосистемам с открытым ключом. - Санкт-Петербург : БХВ-Петербург, 2007. - 298с. - (Учебное пособие). - Библиогр.: с. 293-298. - На обл.: Математ.минимум.... - ISBN 5-9775-0024-6 : (в пер.) : 298.00.с.	7	
Молдовян Н.А. Введение в криптосистемы с открытым ключом : учебное пособие. - Санкт-Петербург : БХВ-Петербург, 2005. - 286с. - (Учебное пособие). - Библиогр.: с. 283-286. - ISBN 5-94157-563-7 : (в пер.) : 188.00	5	
Электронные ресурсы		
Антивирусная защита компьютерных систем / НОУ «ИНТУИТ», 2003 – 2020.. — Текст : электронный //Национальный Открытый Университет «ИНТУИТ» [сайт]. — URL: http://www.intuit.ru/studies/courses/2259/155/info / (дата обращения: 05.04.2023).		
Безопасность сетей / НОУ «ИНТУИТ», 2003 – 2020.. — Текст : электронный //Национальный Открытый Университет «ИНТУИТ» [сайт]. — URL: http://www.intuit.ru/studies/courses/102/102/info / (дата обращения: 05.04.2023)..		
Введение в защиту информации от внутренних ИТ-угроз / НОУ «ИНТУИТ», 2003 – 2020.. — Текст : электронный //Национальный Открытый Университет «ИНТУИТ» [сайт]. — URL: http://www.intuit.ru/studies/courses/1013/172/info / (дата обращения: 05.04.2023).		
Вирусы и средства борьбы с ними/ НОУ «ИНТУИТ», 2003 – 2020.. — Текст : электронный //Национальный Открытый Университет «ИНТУИТ» [сайт]. — URL: http://www.intuit.ru/studies/courses/1042/154/info / (дата обращения: 05.04.2023).		

Криптографические основы безопасности / НОУ «ИНТУИТ», 2003 – 2020.. — Текст : электронный //Национальный Открытый Университет «ИНТУИТ» [сайт]. — URL: http://www.intuit.ru/studies/courses/28/28/info / (дата обращения: 05.04.2023).		
Математика криптографии и теория шифрования безопасности / НОУ «ИНТУИТ», 2003 – 2020.. — Текст : электронный //Национальный Открытый Университет «ИНТУИТ» [сайт]. — URL: http://www.intuit.ru/studies/courses/552/408/info / (дата обращения: 05.04.2023).		
Основы информационной безопасности / НОУ «ИНТУИТ», 2003 – 2020.. — Текст : электронный //Национальный Открытый Университет «ИНТУИТ» [сайт]. — URL: http://www.intuit.ru/studies/courses/10/10/info / (дата обращения: 05.04.2023).		
ISO27000.RU (ЗАЩИТА-ИНФОРМАЦИИ.SU) // 2007 – 2020.. — Текст : электронный //Информационно-аналитический ресурс [сайт]. — URL: http://www.iso27000.ru/(дата обращения: 05.04.2023)..		
Securitylab.ru // 2007 – 2020.. — Текст : электронный //Информационный портал по безопасности [сайт]. — URL: :https://www.securitylab.ru (дата обращения: 05.04.2023).		
Информационная безопасность. Защита информации // 2007 – 2020.. — Текст : электронный //Информационный портал по безопасности [сайт]. — URL: http://all-ib.ru/, (дата обращения: 05.04.2023).		
Научный журнал «Вопросы кибербезопасности» // 2013 – 2020.. — Текст : электронный // **Scientific, periodic, information-methodicalmagazine** [сайт]. — URL: http://cyberrus.com/ (дата обращения: 05.04.2023).		
Антивирусная защита компьютерных систем / НОУ «ИНТУИТ», 2003 – 2020.. — Текст : электронный //Национальный Открытый Университет «ИНТУИТ» [сайт]. — URL: http://www.intuit.ru/studies/courses/2259/155/info / (дата обращения: 05.04.2023).		

Таблица 3 – Информационное обеспечение

Наименование ресурса **Профессиональные базы данных**	**Договор**	**Срок договора**
База данных электронной библиотечной системы вуза «Электронный читальный зал-БиблиоТех» https://www.novsu.ru/dept/1114/bibliotech/	Договор от 17.12.2014 № БТ-46/11	бессрочный
Электронный каталог научной библиотеки http://mars.novsu.ac.ru/MarcWeb/	База собственной генерации	бессрочный
База данных «Аналитика» (картотека статей) http://mars.novsu.ac.ru/MarcWeb/	База собственной генерации	бессрочный
ЭБС «Электронная библиотечная система Новгородского государственного университета» (ЭБС НовГУ). Универсальный ресурс. Внутривузовские издания НовГУ.	Договор № 230 от 30.12.2022 с ООО «КДУ»	бессрочный
ЭБС «Лань» Единая профессиональная база данных для классических вузов – Издательство Лань «ЭБС» ЭБС ЛАНЬ	Договор от 23.12.2022 № 28/ЕП(У)22 с ООО «Издательство ЛАНЬ»	01.01.2023-31.12.2023
ЭБС «ЛАНЬ» Коллекции: «Физика – Издательство МГТУ им. Н.Э.Баумана», «Информатика - Издательство ДМК Пресс»	Договор от 23.12.2022 № 27/ЕП(У)22 с ООО «ЭБС ЛАНЬ»	01.01.2023-31.12.2023
ЭБС «ЛАНЬ» Универсальный ресурс	Договор от 09.11.2020 № СЭБ НВ–283 с ООО «ЭБС ЛАНЬ»	09.11.2020 - 31.12.2023

Наименование ресурса	Договор	Срок договора
Профессиональные базы данных		
«ЭБС ЮРАЙТ www.biblio-online.ru» Универсальный ресурс.	Договор от 23.12.2022 № 25/ЕП(У)22 с ООО «Электронное издательство ЮРАЙТ»	01.01.2023 - 31.12.2023
«Национальная электронная библиотека» Универсальный ресурс.	Договор от 14.03.2022 № 101/НЭБ/2338-п с ФБГУ «Российская Государственная библиотека»	14.03.2022 - 14.03.2027
ЭБС «IPRsmart» Универсальный ресурс.	Лицензионный договор № 741/22П с ООО Компания «Ай Пи Ар Медиа»	01.01.2023 - 01.01.2024
Универсальная база данных «УБД» Универсальная справочно-информационная полнотекстовая база данных периодических изданий с архивом.	Договор от 30.01.2023 № 01/БВ с ООО «ИВИС»	01.01.2023 - 31.12.2023
Президентская библиотека им. Б. Н. Ельцина https://www.prlib.ru/	в открытом доступе	-
База данных Научной электронной библиотеки eLIBRARY.RU https://elibrary.ru/	в открытом доступе	-
База данных профессиональных стандартов Министерства труда и социальной защиты РФ http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/	в открытом доступе	-
Базы данных Министерства экономического развития РФ	в открытом доступе	-
База данных электронно-библиотечной системы «Национальная электронная библиотека»	в открытом доступе	-
Информационные справочные системы		
Университетская информационная система «РОССИЯ» https://uisrussia.msu.ru	в открытом доступе	-
Национальный портал онлайн обучения «Открытое образование» https://openedu.ru	в открытом доступе	-
Портал открытых данных Российской Федерации https://data.gov.ru	в открытом доступе	-
База открытых данных Министерства труда и социальной защиты РФ https://rosmintrud.ru/opendata	в открытом доступе	-
Справочно-правовая система КонсультантПлюс (КонсультантПлюс студенту и преподавателю) www.consultant.ru/edu/	в открытом доступе	-

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Новгородский государственный университет имени Ярослава Мудрого»
Институт электронных и информационных систем
Кафедра прикладной математики и информатики

УТВЕРЖДАЮ
Директор ИЭИС
_____ В. А. Шульцев
подпись
«14» 05 2023 г.

РАБОЧАЯ ПРОГРАММА
учебной дисциплины (модуля)
Методы защиты информации
по направлению подготовки
01.04.02 - Прикладная математика и информатика

направленности (профилю)
Прикладной анализ данных

СОГЛАСОВАНО
Начальник ООД ИЭИС
_____ И. Н. Гуркова
(подпись)
«14» 05 2023 г.
число месяц

Разработал
доцент кафедры ПМИ
_____ Т. В. Жгун
«17» 05 2023 г.

Принято на заседании кафедры ПМИ
Протокол № 9 от 18. 05 .2023 г.
Заведующий кафедрой ПМИ
_____ В. А. Едемский

ПриложениеВ
(обязательное)

Лист актуализации рабочей программы
учебной дисциплины «Методы защиты информации»

Рабочая программа актуализирована на 20_____/20_____ учебный год.

Протокол № _____ заседания кафедры от «_____»_____ 20_____ г.

Разработчик: _____

Зав. кафедрой_____

Рабочая программа актуализирована на 20____/20____ учебный год.

Протокол № _____ заседания кафедры от «_____»_____ 20_____ г.

Разработчик: _____

Зав. кафедрой_____

Рабочая программа актуализирована на 20____/20____ учебный год.

Протокол № _____ заседания кафедры от «_____»_____ 20_____ г.

Разработчик: _____

Зав. кафедрой_____

Перечень изменений, внесенных в рабочую программу:

Номер изменения	№ и дата протокола заседания кафедры	Содержание изменений	Зав.кафедрой	Подпись