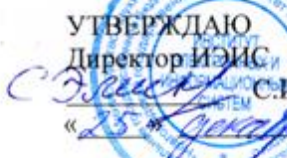


Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новгородский государственный университет имени Ярослава Мудрого»
Институт электронных и информационных систем
Кафедра информационных технологий и систем

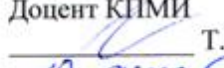
УТВЕРЖДАЮ
Директор ИЭИС
 С.И. Эминов
«25» декабря 2020 г.

РАБОЧАЯ ПРОГРАММА
учебной дисциплины

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

по направлению подготовки
09.03.01 Информатика и вычислительная техника
Направленность (профиль) Программное обеспечение вычислительной техники и
автоматизированных систем

СОГЛАСОВАНО
Зам. директора ИЭИС
 Е.А. Ариас
«21» декабря 2020 г.

Разработал
Доцент КПМИ
 Т.В. Жгун
«10» декабря 2020 г.

Принято на заседании КИТС
Протокол № 4 от 14.12.2020 г.
Заведующий кафедрой, проф.
 Р.В. Петров
«14» декабря 2020 г.

1 Цели и задачи освоения учебной дисциплины

Цель освоения учебной дисциплины: ознакомление с организационными, техническими, алгоритмическими и другими методами и средствами защиты компьютерной информации, с законодательством и стандартами в этой области, с современными криптосистемами.

Задачи:

- сформировать взгляд на криптографию и защиту информации как на систематическую научно-практическую деятельность, носящую прикладной характер;
- сформировать базовые теоретические понятия, лежащие в основе процесса защиты информации;
- дать представление о роли компьютера, как о центральном месте в области криптографии, взявшем на себя большинство функций традиционной компьютерной деятельности, включающей реализацию криптографических алгоритмов, проверку их качества, генерацию и распределение ключей, автоматизацию работы по анализу перехвата и раскрытию шифров;
- научить использованию криптографических алгоритмов в широко распространенных программных продуктах.

2 Место учебной дисциплины в структуре ОПОП

Учебная дисциплина относится к части, формируемой участниками образовательных отношений, учебного плана основной профессиональной образовательной программы направления подготовки 09.03.01 Информатика и вычислительная техника и направленности (профилю) Программное обеспечение вычислительной техники и автоматизированных систем (далее – ОПОП).

В качестве входных требований выступают сформированные ранее компетенции обучающихся, приобретенные ими в рамках изучения следующих дисциплин: «Информатика», «Математика», «Основы программирования: Алгоритмические языки и программирование».

Освоение учебной дисциплины является компетентностным ресурсом при написании выпускной квалификационной работы и дальнейшем обучении в магистратуре.

3 Требования к результатам освоения учебной дисциплины

Перечень компетенций, которые формируются в процессе освоения учебной дисциплины:

профессиональные:

- ПК-2 Способен осуществлять концептуальное, функциональное и логическое проектирование систем среднего и крупного масштаба и сложности.

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)		
	ПК-2.3-1 Знать методы планирования проектных работ; ПК-2.3-2 Знать методы целеполагания;	ПК-2.У-1 Уметь планировать проектные работы; ПК-2.У-2 Уметь разрабатывать технико-экономическое обоснование	ПК-2.В-1 Владеть навыками планирования проектных работ; ПК-2.В-2 Владеть навыками разработки технико-
ПК-2 Способен осуществлять концептуальное, функциональное и логическое проектирование систем среднего и крупного			

масштаба и сложности	ПК-2.3-3 Знать методы концептуального проектирования		экономического обоснования
----------------------	--	--	----------------------------

4 Структура и содержание учебной дисциплины

4.1 Трудоемкость учебной дисциплины

Таблица 2 – Трудоемкость учебной дисциплины для очной формы обучения

Части учебной дисциплины (модуля)	Всего	Распределение по семестрам
		6 семестр
1. Трудоемкость учебной дисциплины (модуля) в зачетных единицах (ЗЕТ)	4	4
2. Контактная аудиторная работа в академических часах (АЧ)	56	56
3. Курсовая работа/курсовой проект (АЧ) (при наличии)	-	-
4. Внеаудиторная СРС в академических часах (АЧ)	88	88
5. Промежуточная аттестация (зачет; дифференцированный зачет; экзамен) (АЧ)	ДЗ	ДЗ

Таблица 3 – Трудоемкость учебной дисциплины для заочной формы обучения

Части учебной дисциплины (модуля)	Всего	Распределение по семестрам	
		7 семестр	8 семестр
1. Трудоемкость учебной дисциплины (модуля) в зачетных единицах (ЗЕТ)	4		4
2. Контактная аудиторная работа в академических часах (АЧ)	16	2	12
3. Курсовая работа/курсовой проект (АЧ) (при наличии)	-		-
4. Внеаудиторная СРС в академических часах (АЧ)	128		128
5. Промежуточная аттестация (зачет; дифференцированный зачет; экзамен) (АЧ)	ДЗ	ДЗ	

4.2 Содержание учебной дисциплины

Тема 1. Введение.

Тема 2. Традиционное шифрование: классические методы.

Тема 3. Алгоритмы симметричного шифрования.

Тема 4. Асимметричные системы шифрования.

Тема 5. Хэш-функции и аутентификация сообщений.

Тема 6. Цифровая подпись.

Тема 7. Криптография с использованием эллиптических кривых.

Тема 8. Безопасность современных сетевых технологий.

4.3 Трудоемкость разделов учебной дисциплины и контактной работы

Таблица 4 – Трудоемкость разделов учебной дисциплины для очной формы обучения

№	Наименование разделов (тем) учебной дисциплины (модуля), УЭМ, наличие КП/КР	Контактная работа (в АЧ)				Внеауд. СРС (в АЧ)	Формы текущего контроля
		Аудиторная			В т.ч. СРС		
		ЛЕК	ПЗ	ЛР			
1.	Тема 1. Введение	1			1	11	

2.	Тема 2. Традиционное шифрование: классические методы	2		8	1	11	Лабораторная работа № 1
3.	Тема 3. Алгоритмы симметричного шифрования	2		9	1	11	Лабораторная работа № 2, опрос
4.	Тема 4. Асимметричные системы шифрования	2		9	1	11	Лабораторная работа № 2
5.	Тема 5. Хэш-функции и аутентификация сообщений	2		8	1	11	Лабораторная работа № 3, опрос
6.	Тема 6. Цифровая подпись	1		8	1	11	Лабораторная работа № 4
7.	Тема 7. Криптография с использованием эллиптических кривых	2			1	11	Опрос
8.	Тема 8. Безопасность современных сетевых технологий	2			1	11	
	Промежуточная аттестация						<i>дифференцированный зачет</i>
	ИТОГО	14	-	42	8	88	

Таблица 5 – Трудоемкость разделов учебной дисциплины для заочной формы обучения

Таблица 5 – Грудоспособность разделов учебной дисциплины для заочной формы обучения							
№	Наименование разделов (тем) учебной дисциплины (модуля), УЭМ, наличие КП/КР	Контактная работа (в АЧ)			Внеауд. СРС (в АЧ)	Формы текущего контроля	
		Аудиторная					В т.ч. СРС
		ЛЕК	ПЗ	ЛР			
1.	Тема 1. Введение	0,5				16	
2.	Тема 2. Традиционное шифрование: классические методы	0,5		2		16	Лабораторная работа № 1
3.	Тема 3. Алгоритмы симметричного шифрования	0,5		3		16	Лабораторная работа № 2, опрос
4.	Тема 4. Асимметричные системы шифрования	0,5		3		16	Лабораторная работа № 2
5.	Тема 5. Хэш-функции и аутентификация сообщений	0,5		2		16	Лабораторная работа № 3, опрос
6.	Тема 6. Цифровая подпись	0,5		2		16	Лабораторная работа № 4
7.	Тема 7. Криптография с использованием эллиптических кривых	0,5				16	Опрос
8.	Тема 8. Безопасность современных сетевых технологий	0,5				16	
	Промежуточная аттестация						<i>дифференцированный зачет</i>
	ИТОГО	4	-	12	0	128	

4.4 Лабораторные работы и курсовые работы/курсовые проекты

4.4.1 Перечень тем лабораторных работ:

4.4.1.1 Разработка программного макета шифрования информации методами традиционного шифрования. Генерация псевдослучайных последовательностей чисел в системах защиты информации.

4.4.1.2 Изучение стандарта шифрования данных DES. Изучение стандарта

шифрования данных ГОСТ 28147-89.

4.4.1.3 Разработка программного макета шифрования упрощённой модели системы шифрования данных типа RSA. Алгоритм шифрования Диффи-Хеллмана.

4.4.1.4 Однонаправленные хэш-функции. Изучение алгоритмов электронной цифровой подписи в системах защиты информации.

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 6 – Методические рекомендации по организации лекций

№	Темы лекционных занятий (форма проведения)	Трудоемкость в АЧ
1.	Введение. 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. (вводная лекция)	1/0,5
№	Темы лекционных занятий (форма проведения)	Трудоемкость в АЧ
2.	Тема 2. 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 (информационная лекция)	2/0,5
3.	Тема 3. 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 алгоритмов DES и тройного DES. Алгоритмы симметричного шифрования Blowfish, IDEA, ГОСТ 28147, а также режимы их выполнения. Различные способы создания псевдослучайных чисел. AES. Алгоритмы Rijndael и RC6. Математические понятия, лежащие в основе алгоритма Rijndael. Структура шифра (информационная лекция)	2/0,5
4.	Тема 4. Асимметричные системы шифрования Понятия однонаправленной функции и однонаправленной функции с лазейкой. Функции дискретного логарифмирования и основанные на ней алгоритмы: схема Диффи — Хеллмана, схема Эль-Гамала. Схема RSA: алгоритм шифрования, его обратимость, вопросы стойкости (информационная лекция)	2/0,5
5.	Тема 5. 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 (информационная лекция)	2/0,5
6.	Тема 6. Цифровая подпись Основные требования к цифровым подписям, прямая и арбитражная цифровая подпись, стандарты цифровой подписи ГОСТ 3410 и DSS (информационная лекция)	1/0,5
7.	Тема 7. Криптография с использованием эллиптических кривых	2/0,5

	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 (информационная лекция)	
8.	Тема 8. Безопасность современных сетевых технологий Основные протоколы аутентификации и обмена ключей с использованием третьей доверенной стороны. Протоколы аутентификации с использованием поппе и временных меток (информационная лекция)	2/0,5
	ИТОГО	14/4

Рекомендации по проведению лабораторных занятий

Цель лабораторных занятий – научиться решать задачи по защите информации.

Рекомендации по самостоятельной работе

Самостоятельная работа включает разработку программного кода реализации алгоритмов защиты информации.

Содержание тем, для самостоятельного изучения:

- Тема 3. Алгоритмы симметричного шифрования.
Алгоритмы симметричного шифрования Blowfish, IDEA, а также режимы их выполнения. Различные способы создания псевдослучайных чисел. Алгоритм RC6;
- Тема 5. Хэш-функции и аутентификация сообщений.
Сильные хэш-функции SHA-1, SHA-2 и ГОСТ 3411.
- Тема 7. Криптография с использованием эллиптических кривых.
Аналог алгоритма цифровой подписи на эллиптических кривых и алгоритма шифрования с открытым ключом получателя на эллиптических кривых.

6 Фонд оценочных средств учебной дисциплины

Фонд оценочных средств представлен в приложении А.

7 Условия освоения учебной дисциплины

7.1 Учебно-методическое обеспечение

Учебно-методическое обеспечение учебной дисциплины представлено в приложении Б.

7.2 Материально-техническое обеспечение

Таблица 7 – Материально-техническое обеспечение учебной дисциплины

№	Требование к материально-техническому обеспечению согласно ФГОС ВО	Наличие материально-технического оборудования
1.	Учебные аудитории для проведения учебных занятий	аудитория для проведения лекционных и/или практических занятий: учебная мебель (столы, стулья, доска) компьютерный класс с выходом в Интернет, в том числе для проведения практических занятий

		помещения для самостоятельной работы (наличие компьютера, выход в Интернет)	
2.	Мультимедийное оборудование	проектор, компьютер, экран, интерактивная доска	
3.	Программное обеспечение		
Наименование программного продукта		Обоснование для использования (лицензия, договор, счёт, акт или иное)	Дата выдачи
Microsoft Windows 7 Professional		Dreamspark (Imagine) № 370aef61-476a-4b9f-bd7c-84bb13374212	30.04.2015
Microsoft Windows 10 for Educational Use		Dreamspark (Imagine) № 370aef61-476a-4b9f-bd7c-84bb13374212	30.04.2015
Microsoft Office 2013 Standard		Open License № 62018256	31.07.2016
Microsoft Imagine (Microsoft Azure Dev Toolsfor Teaching) Standard		Договор №243/ю, 370aef61-476a-4b9f-bd7c-84bb13374212	19.12.2018
ABBYY FineReader PDF 15 Business. Версия для скачивания (годовая лицензия с академической скидкой)*		Договор №191/Ю	16.11.2020
Kaspersky Endpoint Security для бизнеса – Стандартный Russian Edition. 500-999. Node 1 year Educational Renewal License *		Договор №148/ЕП(У)20-ВБ, 1С1С-200914-092322-497-674	11.09.2020
Антиплагиат. Вуз.*		Договор №3341/12/ЕП(У)21-ВБ	29.01.2021
Подписка Microsoft Office 365		свободно распространяемое для вузов	-
Adobe Acrobat		свободно распространяемое	-
Teams		свободно распространяемое	-
Skype		свободно распространяемое	-
Zoom		свободно распространяемое	-

* отечественное производство

Приложение А
(обязательное)

Фонд оценочных средств
учебной дисциплины «Методы защиты информации»

1 Структура фонда оценочных средств

Фонд оценочных средств состоит из:

- открытой части – это 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;

- закрытой части – это фонд вопросов и заданий, которая не может быть заранее доступна для обучающихся (экзаменационные билеты, вопросы к контрольной работе и пр.) и которая хранится на кафедре.

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.	Лабораторные работы (4 шт.)	Тема 2, Темы 3 – 6	35х4	ПК-2
2.	Опрос по самостоятельной работе	Темы 3, 5, 7	20х3	
<i>Промежуточная аттестация</i>				
	Дифференцированный зачет		-	
	ИТОГО		200	

3 Рекомендации к использованию оценочных средств

1) Опрос

Критерии оценки	Количество вопросов в задании
Количество правильных ответов	3
Полнота ответов	
Понимание излагаемого материала	

Вопросы к опросу по самостоятельной работе:

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-Гамала.

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

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-Гамала.

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 поппе и временных меток.

22 Криптографические 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 Виженера, использующей простой XOR. Метод бесключевого чтения RSA. Атака на подпись RSA по выбранному шифротексту. Вскрытие хэш-функций с использованием парадокса дня рождения.

25 Криптосистемы на эллиптических кривых.

2) Лабораторная работа

Критерии оценки	Количество вариантов заданий
Правильность выполнения лабораторной работы	1
Полнота ответов на защите	

Приложение Б
(обязательное)
Карта учебно-методического обеспечения
учебной дисциплины «Методы защиты информации»

Таблица Б.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		
1 Мельников В. П. Защита информации : учебник : для бакалавров / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; под редакцией 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	4	
2 Гашков С. Б. Криптографические методы защиты информации : учебное пособие для вузов / С. Б. Гашков, Э. А. Применко, М. А. Черепнев. - Москва : Академия, 2010. - 297, [2] с. : ил. - (Высшее профессиональное образование, Информационная безопасность). - Библиогр.: с. 287-294. - Указ.: с. 285-286. - ISBN 978-5-7695-4962-5	1	ЭБС IPR BOOKS
3 Смарт Н. Криптография / Перевод с английского С.А.Кулешова под редакцией С.К.Ландо. - Москва : Техносфера, 2006. - 525 с. : ил. - (Мир программирования). - Прил.: с. 454-506. - Указ.: с. 534-525. - На корешке: VIII.05. - ISBN 0077099877 (?). - ISBN 5-94836-043-1. - ISBN 978-5-94836-043-0. - ISBN 0077099877	9	
4 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. - 172 с. - Библиогр.: с. 170-172. - ISBN 5-89176-233-1	4	
5 Молдовян Н.А. Введение в криптосистемы с открытым ключом : учебное пособие. - Санкт-Петербург : БХВ-Петербург, 2005. - 286 с. - (Учебное пособие). - Библиогр.: с. 283-286. - ISBN 5-94157-563-7	5	
6 Молдовян Н.А. Практикум по криптосистемам с открытым ключом. - Санкт-Петербург : БХВ-Петербург, 2007. - 298 с. - (Учебное пособие). - Библиогр.: с. 293-298. - На обл.: Математ.минимум.... - ISBN 5-9775-0024-6 : (в пер.)	7	
Электронные ресурсы		
1 Макоха А. Н. Математическая логика и теория алгоритмов : учебное пособие / составители А. Н. Макоха [и др.]. — Ставрополь; СКФУ, 2017. — 418 с. — Текст: электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155290		ЭБС Лань
2 Рагозин Ю. Н. Инженерно-техническая защита информации: учебное пособие по физическим основам образования технических каналов утечки информации и по практикуму оценки их опасности / Ю. Н. Рагозин ; под редакцией Т. С. Кулакова. — Санкт-Петербург : Интермедия, 2018. — 168 с. — ISBN 978-5-4383-0161-5. — Текст : электронный // — URL: https://www.iprbookshop.ru/73641.html		ЭБС IPR BOOKS

Таблица Б.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		
1 Сляров Д.В. Искусство защиты и взлома информации. - Санкт-Петербург : БХВ-Петербург, 2004. - 276 с. : ил. - Библиогр.: с. 273-276. - ISBN 5-94157-331-6	1	
2 Рябо Б.Я. Криптографические методы защиты информации : учебное пособие для вузов. - Москва : Горячая линия-Телеком, 2005. - 229 с. - Библиогр.: с. 218-221. - Указ.: с. 222-226. - ISBN 5-93517-265-8	3	
3 Фомичев В.М. Дискретная математика и криптология : Курс лекций / Под общей редакцией Н.Д.Подуфалова. - Москва : Диалог-МИФИ, 2003. - 397 с. : ил. - Библиогр.: с. 386-390. - Слов.: с. 372-385. - ISBN 5-86404-185-8	1	
4 Танова Э.В. Введение в криптографию: как защитить свое письмо от любопытных : учебное пособие. - Москва : БИНОМ. Лаборатория знаний, 2007. - 79,[1] с. : ил. - (Элективный курс, Информатика). - В выход.дан.в назв.:Элективный курс. - ISBN 978-5-94774-716-4	5	
Танова Э.В. Введение в криптографию: как защитить свое письмо от любопытных : методическое пособие. - Москва : БИНОМ. Лаборатория знаний, 2008. - 47,[1] с. - (Элективный курс, Информатика). - В выход.дан.в назв.:Элективный курс. - ISBN 978-5-94774-717-1	5	
Электронные ресурсы		
1 Внуков А.А. Защита информации : учебное пособие для вузов / А. А. Внуков. – 3-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2021. – 161 с. – (Высшее образование). – ISBN 978-5-534-07248-8. – URL: https://urait.ru/bcode/470131		ЭБС Юрайт

Таблица Б.3 – Информационное обеспечение

Наименование ресурса	Договор	Срок договора
Профессиональные базы данных		
База данных электронной библиотечной системы вуза «Электронный читальный зал-БиблиоТех» https://www.novsu.ru/dept/1114/bibliotech/	Договор № БТ-46/11 от 17.12.2014	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
База данных Научной электронной библиотеки eLIBRARY.RU https://elibrary.ru/	в открытом доступе	-
Национальная подписка в рамках проекта Министерства образования и науки РФ (Госзадание № 4/2017 г.) к наукометрическим БД Scopus и Web of Science https://www.webofscience.com/wos/woscc/basic-search https://www.scopus.com/search/form.uri?display=basic#basic	регистрация (территория вуза)	2022
База данных электронно-библиотечной системы «Национальная электронная библиотека» https://нэб.рф	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	-
Официальный сайт Федерального агентства по техническому регулированию и метрологии http://protect.gost.ru/	в открытом доступе	-

Зав. кафедрой

подпись

И.О.Фамилия

« 10 »

2020 г.

Приложение В
(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 _____

Таблица В.1 – Перечень изменений, внесенных в рабочую программу:

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