

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  
« 18 » 06 20 24 г.  
число месяц

**РАБОЧАЯ ПРОГРАММА**  
учебной дисциплины

**МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ**

по направлению подготовки 01.03.01 Математика  
направленность (профиль) Математика в образовании, фундаментальных и прикладных  
исследованиях

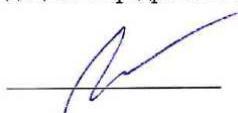
СОГЛАСОВАНО  
Начальник  
Отдела обеспечения деятельности

  
И.Н. Гуркова .  
« 05 » 06 20 24 г.  
число месяц

И.о. зав. выпускающей кафедрой АГ

  
Е.М. Кондрушенко  
« 05 » 06 20 24 г.

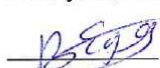
Разработал  
доцент кафедры ПМИ

  
Т.В. Жгун  
« 03 » 05 20 24 г.

Принято на заседании кафедры ПМИ

Протокол № 10 от « 16 » 05 20 24 г.

Заведующий кафедрой ПМИ

  
В.А. Едемский  
« 16 » 05 20 24 г.

## 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 части, формируемой участниками образовательных отношений, учебного плана основной профессиональной образовательной программы основной профессиональной образовательной программы направления подготовки 01.03.01 Математика, направленность (профиль) Математика в образовании, фундаментальных и прикладных исследованиях (далее – ОПОП). В качестве входных требований выступают сформированные ранее компетенции обучающихся, приобретенные ими в рамках следующих дисциплин: «Алгебра», «Алгебра и теория чисел», «Математическая логика», «Основы информатики и программирования», «Математический анализ», «Теория вероятностей и математическая статистика», «Программирование», «Дискретная математика».

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

## 3 Требования к результатам освоения учебной дисциплины

Перечень компетенций, которые формируются в процессе освоения учебной дисциплины:

*Профессиональные компетенции:*

ПК-2 Способен применять основные понятия, идеи и методы фундаментальной математики, современные информационно-коммуникационные технологии в научно-исследовательской деятельности;

ПК-3 Способен к проектированию индивидуальной и совместной научно-исследовательской и учебной деятельности по математике и информатике

Результаты освоения учебной дисциплины представлены в таблице 1.

Таблица 1–Результаты освоения учебной дисциплины

| <i>Код и наименование компетенции</i>                                                                                                                                                | <i>Результаты освоения учебной дисциплины<br/>(индикаторы достижения компетенций)</i>                                                                                                                               |                                                                                                                                                                                                                          |                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| ПК-2<br>Способен применять основные понятия, идеи и методы фундаментальной математики, современные информационно-коммуникационные технологии в научно-исследовательской деятельности | ПК-2.1<br>Знать основные понятия, идеи и методы фундаментальной математики, основы работы компьютеров, технологии программирования, способы оптимизации передачи данных и способы обеспечения безопасности в сетях. | ПК-2.2<br>Уметь составлять математические модели для решения задач в области фундаментальных и прикладных исследований, разрабатывать и применять электронные средства сопровождения научно-исследовательского процесса. | ПК-2.3<br>Владеть техникой составления обзоров, аннотаций, библиографии по тематике проводимых исследований, техникой написания рефератов |
| ПК-3<br>Способен к проектированию индивидуальной и совместной научно-исследовательской и учебной деятельности по математике и информатике                                            | ПК-3.1<br>Знать основы проектной деятельности.                                                                                                                                                                      | ПК-3.2<br>Уметь применять знания в области проектной деятельности к решению профессиональных задач.                                                                                                                      | ПК-3.3<br>Владеть техникой решения проблем, возникающих при осуществлении проектной деятельности.                                         |

#### 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 |
|-----------------------------------------------------------------------------|-------|----------------------------|
|                                                                             |       | 7 семестр                  |
| 1. Трудоемкость учебной дисциплины в зачетных единицах (ЗЕТ)                | 3     | 3                          |
| 2. Контактная аудиторная работа в академических часах (АЧ)                  | 42    | 42                         |
| 3. Курсовая работа/курсовой проект (АЧ) (при наличии)                       | 0     | 0                          |
| 4. Внеаудиторная СРС в академических часах (АЧ)                             | 66    | 66                         |
| 5. Промежуточная аттестация (зачет; дифференцированный зачет; экзамен) (АЧ) | зачет | зачет                      |

4.1.2Трудоемкость 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 односторонней функции и односторонней 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

**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 | Э К 3 |                   |                                            |
|           |                                                                                                 | ЛЕК                     | ПЗ | ЛР |                 |    |       |                   |                                            |
| 8 семестр |                                                                                                 |                         |    |    |                 |    |       |                   |                                            |
| 1         | Введение. Стеганография.                                                                        | 2                       |    |    | 1               |    |       | 6                 |                                            |
| 2         | Традиционное шифрование                                                                         | 3                       | 4  | 6  | 1               |    |       | 15                | Лабораторная работа                        |
| 3         | Алгоритмы симметричного шифрования                                                              | 4                       | 4  | 8  | 1               |    |       | 15                | Лабораторная работа<br>Лабораторная работа |
| 4         | Математические основы криптографии. Системы с открытым ключом                                   | 2                       | 4  | 8  | 1               |    |       | 10                | Лабораторная работа                        |
| 5         | Хэш-функции и аутентификация сообщений. Цифровая подпись                                        | 2                       | 2  | 6  | 1               |    |       | 10                | Лабораторная работа                        |
| 6         | Криптография с использованием эллиптических кривых. Безопасность современных сетевых технологий | 1                       |    |    | 1               |    |       | 10                |                                            |
|           | Промежуточная аттестация                                                                        |                         |    |    |                 |    |       |                   | зачет                                      |

|  |                          |           |          |           |          |  |  |           |  |
|--|--------------------------|-----------|----------|-----------|----------|--|--|-----------|--|
|  | <b>ИТОГО за 7семестр</b> | <b>14</b> | <b>0</b> | <b>28</b> | <b>6</b> |  |  | <b>66</b> |  |
|--|--------------------------|-----------|----------|-----------|----------|--|--|-----------|--|

#### 4.4 Лабораторные работы и курсовые работы/курсовые проекты

4.4.1 Перечень тем лабораторных работ:

1. Традиционное шифрование
2. Стандарты симметричного шифрования. VS-AES
3. Математические основы криптографии
4. Системы с открытым ключом
5. 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

| <i>№</i> | <i>Темы лекционных занятий (форма проведения)</i>                                                                              | <i>Трудоем-<br/>кость в<br/>АЧ</i> |
|----------|--------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
| 1        | Введение. Стеганография (вводная лекция с элементами проблемной лекции)                                                        | 2                                  |
| 2        | Традиционное шифрование(лекция-презентация)                                                                                    | 3                                  |
| 3.       | Алгоритмы симметричного шифрования (проблемная лекция, рефлексия полученных образовательных результатов)                       | 3                                  |
| 4        | Математические основы криптографии. Системы с открытым ключом (лекция-презентация)                                             | 4                                  |
| 5        | Хэш-функции и аутентификация сообщений. Цифровая подпись (проблемная лекция, рефлексия полученных образовательных результатов) | 1                                  |
| 6        | Криптография с использованием эллиптических кривых. Безопасность современных сетевых технологий (лекция-презентация)           | 1                                  |
|          | <b>ИТОГО</b>                                                                                                                   | <b>14</b>                          |

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. Издательство НовГУ . 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 10.11.2023)

## 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 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)<br>помещения для самостоятельной работы (наличие компьютера, выход в Интернет) |             |
| 2.                                                                                                                                      | Мультимедийное оборудование                                        | компьютер, проектор, экран, выход в интернет                                                                                                                                         |             |
| 3.                                                                                                                                      | Программное обеспечение                                            |                                                                                                                                                                                      |             |
| Наименование программного продукта                                                                                                      |                                                                    | Обоснование для использования (лицензия, договор, счёт, акт или иное)                                                                                                                | Дата выдачи |
| ContentReader PDF 15 Business Версия для скачивания (годовая лицензия с академической скидкой) *<br><i>Только для осеннего семестра</i> |                                                                    | Договор №3КС/260                                                                                                                                                                     | 31.10.2023  |
| Антиплагиат. Вуз.*                                                                                                                      |                                                                    | Договор №05//ЕП(У)24-ВБ                                                                                                                                                              | 18.01.2024  |
| MS Office 365                                                                                                                           |                                                                    | Безвозмездно передаваемое ВУЗам                                                                                                                                                      | -           |
| Adobe Acrobat                                                                                                                           |                                                                    | свободно распространяемое                                                                                                                                                            | -           |
| Teams                                                                                                                                   |                                                                    | Входит в состав MS Office 365                                                                                                                                                        | -           |
| Skype                                                                                                                                   |                                                                    | свободно распространяемое                                                                                                                                                            | -           |
| Zoom                                                                                                                                    |                                                                    | свободно распространяемое                                                                                                                                                            | -           |
| "Kaspersky Endpoint Security для бизнеса - Стандартный Russian Education Renewal. 250-499 Node I year License" /1 год *                 |                                                                    | Договор №294/ЕП(У)25-ВБ                                                                                                                                                              | 13.09.2023  |
| Astra Linux Special Edition*                                                                                                            |                                                                    | 195200041-alse-1.7-client-base_orel-x86_64-0-14211                                                                                                                                   | 09.12.2022  |
| Astra Linux Special Edition*                                                                                                            |                                                                    | 195200041-alse-1.7-client-base_orel-x86_64-0-12617                                                                                                                                   | 21.11.2022  |
| Astra Linux Special Edition*                                                                                                            |                                                                    | 195200041-alse-1.7-client-max-x86_64-0-11416                                                                                                                                         | 26.10.2022  |
| Astra Linux Special Edition*                                                                                                            |                                                                    | 195200041-alse-1.7-client-base_orel-x86_64-0-9651                                                                                                                                    | 28.09.2022  |
| Astra Linux Special Edition*                                                                                                            |                                                                    | 195200041-alse-1.7-client-base-x86_64-0-8801                                                                                                                                         | 07.09.2022  |
| Astra Linux Special Edition*                                                                                                            |                                                                    | 195200041-alse-1.7-client-base-x86_64-0-8590                                                                                                                                         | 01.09.2022  |
| * отечественное производство                                                                                                            |                                                                    |                                                                                                                                                                                      |             |



## Свободно распространяемое программное обеспечение

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

Приложение А  
(обязательное)  
**Фонд оценочных средств**  
**учебной дисциплины «Методы защиты информации»**

### 1 Структура фонда оценочных средств

Фонд оценочных средств состоит из 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                               | Лабораторная работа                      | Традиционное шифрование                    | 30         | ПК-2<br>ПК-3            |
| 2                               | Лабораторная работа                      | Стандарты симметричного шифрования.        | 30         | ПК-2<br>ПК-3            |
| 3                               | Лабораторная работа                      | Математические основы криптографии         | 30         | ПК-2<br>ПК-3            |
| 4                               | Лабораторная работа                      | Системы с открытым ключом                  | 30         | ПК-2<br>ПК-3            |
| 5                               | Лабораторная работа                      | Аутентификация сообщений. Цифровая подпись | 30         | ПК-2<br>ПК-3            |
| <i>Промежуточная аттестация</i> |                                          |                                            |            |                         |
|                                 |                                          |                                            |            |                         |
|                                 | <b>ИТОГО</b>                             |                                            | <b>150</b> |                         |

### 3 Рекомендации к использованию оценочных средств

Таблица А.2 –Лабораторные работы

| <i>Критерии оценки</i>                                           | <i>Количество вариантов заданий</i> | <i>Количество заданий в одном варианте</i> |
|------------------------------------------------------------------|-------------------------------------|--------------------------------------------|
| Соответствие выполненной работы описанию – 6 баллов              | 5                                   | 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 неотвержаемым?
5. Что такое дайджест-сообщение?
6. Что такое вычислительно необратимая функция?

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

Таблица Б.1 – Основная литература

| Библиографическое описание издания<br>(автор, наименование, вид, место и год издания, кол.стр.)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Кол.экз.<br>в библ.<br>НовГУ | Наличие в ЭБС |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|---------------|
| <b>Печатные источники</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                              |               |
| <b>Мельников В. П.</b> 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                            |               |
| <b>Лапони́на О.Р.</b> 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.)<br><br>Лапони́на, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие / О. Р. Лапони́на ; под редакцией В. А. Сухомлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 605 с. — ISBN 978-5-4497-0684-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <a href="https://www.iprbookshop.ru/97571.html">https://www.iprbookshop.ru/97571.html</a> (дата обращения: 19.03.2024). — Режим доступа: для авторизир. пользователей | 1                            | IPR SMART     |
| <b>Электронные ресурсы</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                              |               |
| Методы защиты информации: конспект лекций для специальности 01.03.02 "Прикладная математика и информатика" / сост. Т. В. Жгун. – Великий Новгород, 2016.– 165 с. – Текст: электронный. //ЭБС НовГУ.. –URL: <a href="https://novsu.bookonline.ru/reader/book/2436">https://novsu.bookonline.ru/reader/book/2436</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                              | ЭБС НовГУ     |
| Методы защиты информации :методические указания по практическим занятиям для направления 01.03.02 "Прикладная математика и информатика" / сост. Т. В. Жгун. – Великий Новгород, 2017. – 62 с. – Текст: электронный. //ЭБС НовГУ.. – URL: <a href="https://novsu.bookonline.ru/reader/book/2568">https://novsu.bookonline.ru/reader/book/2568</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                              | ЭБС НовГУ     |
| Методы защиты информации :методические указания к выполнению лабораторных работ для направления 01.03.02 "Прикладная математика и информатика" / сост. Т. В. Жгун. – Великий Новгород, 2017.– 62 с. – Текст: электронный. //ЭБС НовГУ.. –URL: <a href="https://novsu.bookonline.ru/reader/book/2567">https://novsu.bookonline.ru/reader/book/2567</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                              | ЭБС НовГУ     |

Новгородский государственный  
университет им. Ярослава Мудрого  
Научная библиотека  
Сектор учета *Васильев*



Таблица Б.2 – Дополнительная литература

| Библиографическое описание издания<br>(автор, наименование, вид, место и год издания, кол.стр.)                                                                                                                                                                                                             | Кол.экз. в<br>библ.<br>НовГУ | Наличие в<br>ЭБС |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|------------------|
| Печатные источники                                                                                                                                                                                                                                                                                          |                              |                  |
| <b>Рябко Б.Я.</b> 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.                                                                           | 2                            |                  |
| – <b>Рябко Б.Я.</b> 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                | 3                            |                  |
| <b>Молдовян Н.А.</b> 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.                                                               | 1                            |                  |
| <b>Молдовян Н.А.</b> 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                                                                                  | 2                            |                  |
| Электронные ресурсы                                                                                                                                                                                                                                                                                         |                              |                  |
| Антивирусная защита компьютерных систем. – Текст: электронный. //Национальный Открытый Университет «ИНТУИТ», 2003 – 2020.: [сайт]. — URL: <a href="http://www.intuit.ru/studies/courses/2259/155/info">http://www.intuit.ru/studies/courses/2259/155/info</a> / (дата обращения: 05.11.2023).               |                              |                  |
| Безопасность сетей. — Текст : электронный //Национальный Открытый Университет «ИНТУИТ», 2003 – 2020: [сайт]. — URL: <a href="http://www.intuit.ru/studies/courses/102/102/info">http://www.intuit.ru/studies/courses/102/102/info</a> / (дата обращения: 05.11.2023)..                                      |                              |                  |
| Введение в защиту информации от внутренних ИТ-угроз. — Текст : электронный //Национальный Открытый Университет «ИНТУИТ», 2003 – 2020: [сайт]. — URL: <a href="http://www.intuit.ru/studies/courses/1013/172/info">http://www.intuit.ru/studies/courses/1013/172/info</a> / (дата обращения: 05.11.2023).    |                              |                  |
| Вирусы и средства борьбы с ними. — Текст : электронный //Национальный Открытый Университет «ИНТУИТ», 2003 – 2020: [сайт]. — URL: <a href="http://www.intuit.ru/studies/courses/1042/154/info">http://www.intuit.ru/studies/courses/1042/154/info</a> / (дата обращения: 05.11.2023).                        |                              |                  |
| Криптографические основы безопасности. — Текст : электронный //Национальный Открытый Университет «ИНТУИТ», 2003 – 2020: [сайт]. — URL: <a href="http://www.intuit.ru/studies/courses/28/28/info">http://www.intuit.ru/studies/courses/28/28/info</a> / (дата обращения: 05.11.2023).                        |                              |                  |
| Математика криптографии и теория шифрования безопасности. — Текст : электронный //Национальный Открытый Университет «ИНТУИТ», 2003 – 2020: [сайт]. — URL: <a href="http://www.intuit.ru/studies/courses/552/408/info">http://www.intuit.ru/studies/courses/552/408/info</a> / (дата обращения: 05.11.2023). |                              |                  |
| Основы информационной безопасности. — Текст : электронный //Национальный Открытый Университет «ИНТУИТ», 2003 – 2020: [сайт]. — URL: <a href="http://www.intuit.ru/studies/courses/10/10/info">http://www.intuit.ru/studies/courses/10/10/info</a> / (дата обращения: 05.11.2023).                           |                              |                  |

Новгородский государственный  
университет им. Ярослава Мудрого  
Научная библиотека  
Сектор учета

|                                                                                                                                                                                                                                                                                               |  |  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|--|
| ISO27000.RU (ЗАЩИТА-ИНФОРМАЦИИ.SU) , 2007 – 2020.. — Текст : электронный //Информационно-аналитический ресурс :[сайт]. — URL: <a href="http://www.iso27000.ru/">http://www.iso27000.ru/</a> (дата обращения: 05.11.2023)..                                                                    |  |  |
| Securitylab.ru, 2007 – 2020.. — Текст : электронный //Информационный портал по безопасности : [сайт]. — URL: <a href="https://www.securitylab.ru">:https://www.securitylab.ru</a> (дата обращения: 05.11.2023).                                                                               |  |  |
| Информационная безопасность. Защита информации, 2007 – 2020.. — Текст : электронный //Информационный портал по безопасности : [сайт]. — URL: <a href="http://all-ib.ru/">http://all-ib.ru/</a> , (дата обращения: 05.11.2023).                                                                |  |  |
| Вопросы кибербезопасности: научный журнал, 2013 – 2020.. — Текст : электронный // <b>Scientific, periodic, information-methodicalmagazine</b> : [сайт]. — URL: <a href="http://cyberrus.com/">http://cyberrus.com/</a> (дата обращения: 05.11.2023).                                          |  |  |
| Антивирусная защита компьютерных систем . — Текст : электронный //Национальный Открытый Университет «ИНТУИТ», 2003 – 2020: [сайт]. — URL: <a href="http://www.intuit.ru/studies/courses/2259/155/info/">http://www.intuit.ru/studies/courses/2259/155/info/</a> (дата обращения: 05.11.2023). |  |  |

Таблица Б.3 – Информационное обеспечение модуля

| Наименование ресурса                                                                                                                                                            | Договор                                                                             | Срок договора                                                                         |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <b>Электронная библиотека НовГУ</b>                                                                                                                                             |                                                                                     |                                                                                       |
| Электронный каталог научной библиотеки <a href="http://mars.novsu.ac.ru/MarcWeb/">http://mars.novsu.ac.ru/MarcWeb/</a>                                                          | База собственной генерации                                                          | бессрочный                                                                            |
| База данных «Аналитика» (картотека статей) <a href="http://mars.novsu.ac.ru/MarcWeb/">http://mars.novsu.ac.ru/MarcWeb/</a>                                                      | База собственной генерации                                                          | бессрочный                                                                            |
| <b>ЭБС «Электронная библиотечная система Новгородского государственного университета» (ЭБС НовГУ).</b> Универсальный ресурс. Внутривузовские издания НовГУ.                     | Договор № 230 от 30.12.2022 с ООО «КДУ»                                             | бессрочный                                                                            |
| <b>ЭБС «Лань»</b><br>Единая профессиональная база данных для классических вузов – Издательство Лань «ЭБС» <b>ЭБС ЛАНЬ</b>                                                       | Договор № 34/ЕП(Т)23 от 22.12.2023 с ООО «Издательство ЛАНЬ»                        | с 01.01.2024 по 31.12.2024                                                            |
| <b>ЭБС «ЛАНЬ»</b><br>Коллекции: «Физика – Издательство МГТУ им. Н.Э.Баумана», «Информатика - Издательство ДМК Пресс», «Журналистика и медиа-бизнес - Издательство Аспект Пресс» | Договор № 33/ЕП(У)23 от 25.12.2023 с ООО «ЭБС ЛАНЬ»                                 | с 01.01.2024 по 31.12.2024                                                            |
| <b>ЭБС «ЛАНЬ»</b><br>Универсальный ресурс                                                                                                                                       | Договор № СЭБ НВ–283 с ООО «ЭБС ЛАНЬ» от 09.11.2020                                 | с 09.11.2020 по 31.12.2023<br>Договор пролонгирован до 31.12.2024 (основание: п.6.1.) |
| <b>«ЭБС ЮРАЙТ <a href="http://www.biblio-online.ru">www.biblio-online.ru</a>»</b><br>Универсальный ресурс.                                                                      | Договор № 35/ЕП(У)23 от 25.12.2023 с ООО «Электронное издательство ЮРАЙТ»           | с 01.01.2024 по 31.12.2024                                                            |
| <b>«Национальная электронная библиотека»</b><br>Универсальный ресурс.                                                                                                           | Договор №101/НЭБ/2338П от 14.03.2022 с ФБГУ «Российская Государственная библиотека» | с 14.03.2022 по 13.03.2027                                                            |

Новгородский государственный  
университет им. Ярослава Мудрого  
Научная библиотека  
Сектор учета *Колесникова*



| Наименование ресурса                                                                                                                                                                                                                                                                                                              | Договор                                                                                   | Срок договора              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|----------------------------|
| ЭБС «IPRsmart» Универсальный ресурс.                                                                                                                                                                                                                                                                                              | Лицензионный договор № 11040/23П/31/ЕП(У)23 от 22.12.2023 с ООО Компания «Ай Пи Ар Медиа» | с 01.01.2024 по 31.12.2024 |
| ЭБС «IPRsmart»<br>Электронно-образовательный ресурс для иностранных студентов «РУССКИЙ ЯЗЫК КАК ИНОСТРАННЫЙ» (РКИ).                                                                                                                                                                                                               | Договор № 436/ЕП(У)23-ВБ от 15.12.2023 с ООО Компания «Ай Пи Ар Медиа»                    | с 01.01.2024 по 31.01.2025 |
| ЭБС Polpred.com. Обзор СМИ.<br>Электронные статьи 600 деловых газет, журналов, информагентств за 20 лет.                                                                                                                                                                                                                          | Соглашение с ООО «ПОЛПРЕД Справочники». Тестовый доступ.                                  | с 01.01.2023               |
| <b>Профессиональные базы данных</b>                                                                                                                                                                                                                                                                                               |                                                                                           |                            |
| Президентская библиотека им. Б. Н. Ельцина<br><a href="https://www.prilib.ru/">https://www.prilib.ru/</a>                                                                                                                                                                                                                         | в открытом доступе                                                                        | -                          |
| База данных Научной электронной библиотеки eLIBRARY.RU <a href="https://elibrary.ru/">https://elibrary.ru/</a>                                                                                                                                                                                                                    | в открытом доступе                                                                        | -                          |
| База данных профессиональных стандартов Министерства труда и социальной защиты РФ <a href="http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/">http://profstandart.rosmintrud.ru/obshchiy-informatsionnyy-blok/natsionalnyy-reestr-professionalnykh-standartov/</a> | в открытом доступе                                                                        | -                          |
| База данных электронно-библиотечной системы «Национальная электронная библиотека» <a href="https://нэб.рф">https://нэб.рф</a>                                                                                                                                                                                                     | в открытом доступе                                                                        | -                          |
| <b>Информационные справочные системы</b>                                                                                                                                                                                                                                                                                          |                                                                                           |                            |
| Университетская информационная система «РОССИЯ» <a href="https://lib.tysur.ru/ru/resursy/bazy-dannyh/uis-rossiya">https://lib.tysur.ru/ru/resursy/bazy-dannyh/uis-rossiya</a>                                                                                                                                                     | в открытом доступе                                                                        | -                          |
| Национальный портал онлайн обучения «Открытое образование» <a href="https://openedu.ru">https://openedu.ru</a>                                                                                                                                                                                                                    | в открытом доступе                                                                        | -                          |
| Портал открытых данных Российской Федерации <a href="https://data.gov.ru">https://data.gov.ru</a>                                                                                                                                                                                                                                 | в открытом доступе                                                                        | -                          |
| Справочно-правовая система КонсультантПлюс (КонсультантПлюс студенту и преподавателю) <a href="http://www.consultant.ru/edu/">www.consultant.ru/edu/</a>                                                                                                                                                                          | в открытом доступе                                                                        | -                          |

Проверено НБ НовГУ

Новгородский государственный  
университет им. Ярослава Мудрого  
Научная библиотека  
Сектор учета

Зав. кафедрой ПМИ В.А. Едемский  
подпись И.О. Фамилия  
« 16 » 05 2024 г.



[illegible]