|  |  |
| --- | --- |
| Министерство науки и высшего образования Российской Федерации | |
| Федеральное государственное бюджетное образовательное учреждение | |
| высшего образования | |
| «Российский государственный университет им. А.Н. Косыгина | |
| (Технологии. Дизайн. Искусство)» | |
|  | |
| Институт | Мехатроники и информационных технологий |
| Кафедра | Прикладной математики и программирования |

|  |  |  |
| --- | --- | --- |
| **РАБОЧАЯ ПРОГРАММА**  **УЧЕБНОЙ ДИСЦИПЛИНЫ** | | |
| **Методы криптографической защиты информации** | | |
| Уровень образования | бакалавриат | |
| Направление подготовки | 01.03.02 | Прикладная математика и информатика |
| Направленность (профиль) | Математические методы, технологии цифрового моделирования и искусственного интеллекта | |
| Срок освоения образовательной программы по очной форме обучения | 4 года | |
| Форма обучения | очная | |

|  |  |  |
| --- | --- | --- |
| Рабочая программа учебной дисциплины «Методы криптографической защиты информации» основной профессиональной образовательной программы высшего образования*,* рассмотрена и одобрена на заседании кафедры, протокол №10 от 29.06.2021 г. | | |
| Разработчики рабочей программы учебной дисциплины: | | |
|  | Доцент | А.М. Романенков |
|  | Ассистент | А.Т. Костоев |
| Заведующий кафедрой: | | В.В. Горшков |

# ОБЩИЕ СВЕДЕНИЯ

Учебная дисциплина «Методы криптографической защиты информации» изучается в седьмом семестре.

Курсовая работа предусмотрена.

## Форма промежуточной аттестации:

Экзамен.

## Место учебной дисциплины в структуре ОПОП

Учебная дисциплина «Методы криптографической защиты информации» относится к части, формируемой участниками образовательных отношений*.*

Основой для освоения дисциплины являются результаты обучения по предшествующим дисциплинам:

* + - Программирование на платформе Net;
    - Методы программирования цифровых приложений;
    - Теория языков программирования, трансляторов и вычислительных систем.

Результаты освоения учебной дисциплины в дальнейшем будут использованы при прохождении производственной практики и (или) выполнении выпускной квалификационной работы.

# ЦЕЛИ И ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Целями изучения дисциплины «Методы криптографической защиты информации» являются:

* + - изучение современных методов и средств защиты информации;
    - изучение криптографических алгоритмов, используемых в разработке программного обеспечения, направленного на защиту информационных систем;
    - формирование навыков разработки программного обеспечения, направленного на защиту информационных систем;
    - формирование навыков реализации криптографических алгоритмов при разработке программного обеспечения;
    - формирование у обучающихся компетенций, установленных образовательной программой в соответствии с ФГОС ВО по данной дисциплине.

Результатом обучения по учебной дисциплине является овладение обучающимися знаниями, умениями, навыками и опытом деятельности, характеризующими процесс формирования компетенций и обеспечивающими достижение планируемых результатов освоения учебной дисциплины.

## Формируемые компетенции, индикаторы достижения компетенций, соотнесённые с планируемыми результатами обучения по дисциплине:

| **Код и наименование компетенций** | **Код и наименование индикатора**  **достижения компетенций** | **Планируемые результаты обучения**  **по дисциплине** |
| --- | --- | --- |
| ПК-1  Способен проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к информационной системе. | ИД-ПК-1.1  Использование основных алгоритмических и программных решений, связанных с объектами и системами информационных технологий; | * Анализирует и использует при разработке программного обеспечения современные средства защиты информации; * Анализирует средства и методы использования криптографических алгоритмов при разработке программных комплексов в информационной системе; * Использует математические основы криптографии при разработке программного обеспечения; * Реализует криптографические алгоритмы при разработке программного обеспечения. |
| ИД-ПК-1.3  Анализ средств защиты информационных систем и сетей; |
| ИД-ПК-1.4  Анализ и реализация криптографических алгоритмов в современных программных комплексах. |

# СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Общая трудоёмкость учебной дисциплины по учебному плану составляет:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| по очной форме обучения – | 4 | **з.е.** | 144 | **час.** |

## Структура учебной дисциплины для обучающихся по видам занятий

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Структура и объем дисциплины** | | | | | | | | | |
| **Объем дисциплины по семестрам** | **форма промежуточной аттестации** | **всего, час** | **Контактная аудиторная работа, час** | | | | **Самостоятельная работа обучающегося, час** | | |
| **лекции, час** | **практические занятия, час** | **лабораторные занятия, час** | **практическая подготовка, час** | **курсовая работа** | **самостоятельная работа обучающегося, час** | **промежуточная аттестация, час** |
| 7 семестр | экзамен, курсовая работа | 144 | 30 | 45 |  |  | 18 | 15 | 36 |
| Всего: |  | 144 | 30 | 45 |  |  | 18 | 15 | 36 |

## Структура учебной дисциплины для обучающихся по разделам и темам дисциплины:

| **Планируемые (контролируемые) результаты освоения:**  **код(ы) формируемой(ых) компетенции(й) и индикаторов достижения компетенций** | **Наименование разделов, тем;**  **форма(ы) промежуточной аттестации** | **Виды учебной работы** | | | | **Самостоятельная работа, час** | **Виды и формы контрольных мероприятий, обеспечивающие по совокупности текущий контроль успеваемости;**  **формы промежуточного контроля успеваемости** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Контактная работа** | | | |
| **Лекции, час** | **Практические занятия, час** | **Лабораторные работы, час** | **Практическая подготовка, час** |
|  | **Седьмой семестр** | | | | | | |
| ПК-1:  ИД-ПК-1.1  ИД-ПК-1.3  ИД-ПК-1.4 | **Раздел I. Математические основы криптографии** | х | х | х | х | 7 | Формы текущего контроля  по разделу I:  самостоятельные проверочные работы |
| Тема 1.1  Арифметика остатков. | 2 |  |  |  | х |
| Тема 1.2  Конечные поля. | 2 |  |  |  | х |
| Тема 1.3  Основные алгоритмы. | 2 |  |  |  | х |
| Тема 1.4  Вероятность. | 2 |  |  |  | х |
| Тема 1.5  Эллиптические кривые. | 2 |  |  |  | х |
| Практическое занятие № 1.1  Арифметика остатков. |  | 4 |  |  | х |
| Практическое занятие № 1.2  Конечные поля. |  | 4 |  |  | х |
| Практическое занятие № 1.3  Основные алгоритмы. |  | 4 |  |  | x |
| Практическое занятие № 1.4  Вероятность. |  | 4 |  |  | x |
| Практическое занятие № 1.5  Эллиптические кривые. |  | 4 |  |  | х |
| **Раздел II. Алгоритмы шифрования** | х | х | х | х | 8 | Формы текущего контроля  по разделу II:  самостоятельные проверочные работы |
| Тема 2.1  Исторические шифры. | 4 |  |  |  | х |
| Тема 2.2  Симметричные шифры. | 4 |  |  |  | х |
| Тема 2.3  Распределение симметричных ключей. | 4 |  |  |  | х |
| Тема 2.4  Основные алгоритмы шифрования с открытым ключом. | 4 |  |  |  | х |
| Тема 2.5  Распределение ключей, схемы подписей  и хэш-функции. | 4 |  |  |  | х |
| Практическое занятие № 2.1  Исторические шифры. |  | 5 |  |  | х |
| Практическое занятие № 2.2  Симметричные шифры. |  | 5 |  |  | x |
| Практическое занятие № 2.3  Распределение симметричных ключей. |  | 5 |  |  | x |
| Практическое занятие № 2.4  Основные алгоритмы шифрования с открытым ключом. |  | 5 |  |  | x |
| Практическое занятие № 2.5  Распределение ключей, схемы подписей  и хэш-функции. |  | 5 |  |  | х |
| Выполнение курсовой работы | х | х | х | х | 18 | защита курсовой работы |
| Экзамен | х | х | х | х | 36 | экзамен по билетам |
| **ИТОГО за седьмойсеместр** | **30** | **45** |  |  | **69** |  |
| **ИТОГО за весь период** | **30** | **45** |  |  | **69** |  |

## Краткое содержание учебной дисциплины

|  |  |  |
| --- | --- | --- |
| **№ пп** | **Наименование раздела и темы дисциплины** | **Содержание раздела (темы)** |
| **Раздел I** | **Математические основы криптографии** | |
| Тема 1.1 | Арифметика остатков | Битовые операции. Получение, изменение заданного бита в n-битном слове. Манипуляции с битами в слове: перестановка, «xor» битов и т.д. Основные алгебраические структуры: группы, кольца, поля. Кольца вычетов. Арифметические операции в кольцах вычетов. Критерий обратимости элемента в кольце вычетов. Алгоритм возведения в степень в кольце вычетов. Функция Эйлера и ее свойства. Приведенная система вычетов. Теорема Эйлера. Малая теорема Ферма и её роль в тестах на простоту числа. Наибольший общий делитель. Алгоритм Евклида и расширенный алгоритм Евклида. Поиск обратного элемента. Китайская теорема об остатках. Делимость в кольцах. Основные признаки делимости. Конечные поля. Пример GF(2), GF(256). Вычисление обратного элемента в GF(256). Проверка числа на простоту. Дискретные логарифмы. Сверхвозрастающие последовательности. Задача об укладке ранца. Применение в криптографии. |
| Тема 1.2 | Конечные поля |
| Тема 1.3 | Основные алгоритмы |
| Тема 1.4 | Вероятность |
| Тема 1.5 | Эллиптические кривые |
| **Раздел II** | **Алгоритмы шифрования** | |
| Тема 2.1 | Исторические шифры. | Алгоритм RC4. Классификация шифров. Алгоритм DES. Режимы сцепления блоков шифротекста. Алгоритм RSA. Алгоритм Rijndael. Алгоритм ГОСТ. Алгоритм Serpent. Алгоритм Mars. Алгоритм Twofish. Алгоритм Blowfish. Алгоритм RC6. Проверка числа на простоту. Хэш-функции. Схема Эль-Гамаля и шифрование Эль-Гамаля. Цифровая подпись и проверка подлинности. Генераторы псевдослучайных чисел. Основные понятия криптоанализа. Типы атак. Понятие надежности алгоритма. Взлом простых шифров: xor и шифр Цезаря. Стандартные Crypto API ОС Unix. Стандартные Crypto API Windows. Crypto API .NET Framework 4.0. |
| Тема 2.2 | Симметричные шифры. |
| Тема 2.3 | Распределение симметричных ключей. |
| Тема 2.4 | Основные алгоритмы шифрования с открытым ключом. |
| Тема 2.5 | Распределение ключей, схемы подписей  и хэш-функции. |

## Организация самостоятельной работы обучающихся

Самостоятельная работа студента – обязательная часть образовательного процесса, направленная на развитие готовности к профессиональному и личностному самообразованию, на проектирование дальнейшего образовательного маршрута и профессиональной карьеры.

Самостоятельная работа обучающихся по дисциплине организована как совокупность аудиторных и внеаудиторных занятий и работ, обеспечивающих успешное освоение дисциплины.

Аудиторная самостоятельная работа обучающихся по дисциплине выполняется на учебных занятиях под руководством преподавателя и по его заданию*.* Аудиторная самостоятельная работа обучающихся входит в общий объем времени, отведенного учебным планом на аудиторную работу, и регламентируется расписанием учебных занятий.

Внеаудиторная самостоятельная работа обучающихся – планируемая учебная, научно-исследовательская, практическая работа обучающихся, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия, расписанием учебных занятий не регламентируется.

Внеаудиторная самостоятельная работа обучающихся включает в себя:

изучение теоретического и практического материала по рекомендованным источникам;

выполнение самостоятельных работ;

выполнение курсовой работы;

подготовка к промежуточной аттестации в течение семестра*.*

## Применение электронного обучения, дистанционных образовательных технологий

При реализации программы учебной дисциплины электронное обучение и дистанционные образовательные технологии не применяются.

# РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, КРИТЕРИИ ОЦЕНКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ, СИСТЕМА И ШКАЛА ОЦЕНИВАНИЯ

## Соотнесение планируемых результатов обучения с уровнями сформированности компетенции.

|  |  |  |  |
| --- | --- | --- | --- |
| **Уровни сформированности компетенции(-й)** | **Итоговое количество баллов**  **в 100-балльной системе**  **по результатам текущей и промежуточной аттестации** | **Оценка в пятибалльной системе**  **по результатам текущей и промежуточной аттестации** | **Показатели уровня сформированности**  **профессиональной(-ых)**  **компетенции(-й)** |
| ПК-1:  ИД-ПК-1.1  ИД-ПК-1.3  ИД-ПК-1.4 |
| высокий |  | отлично | Обучающийся:   * исчерпывающе и логически стройно излагает учебный материал, умеет связывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения; * в полной мере применяет изученные методы и средства защиты информации при решении поставленных задач; * показывает высокий уровень понимания работы криптографических алгоритмов и способен применять их при решении поставленных задач; * демонстрирует высокий уровень программирования и разработки программного обеспечения в области защиты информации; * свободно ориентируется в учебной и профессиональной литературе; * дает развернутые, исчерпывающие, профессионально грамотные ответы на вопросы, в том числе, дополнительные. |
| повышенный |  | хорошо | Обучающийся:   * достаточно подробно, грамотно и по существу излагает изученный материал, приводит и раскрывает в тезисной форме основные понятия; * использует базовые методы и средства защиты информации при решении поставленных задач; * показывает базовый уровень понимания работы криптографических алгоритмов и способен применять их при решении поставленных задач; * демонстрирует достаточно хороший уровень программирования и разработки программного обеспечения в области защиты информации; * достаточно хорошо ориентируется в учебной и профессиональной литературе; * дает ответы на поставленные вопросы, отражающие знания теоретического материала, при этом, не допуская существенных неточностей. |
| базовый |  | удовлетворительно | Обучающийся:   * демонстрирует теоретические знания основного учебного материала дисциплины в объеме, необходимом для дальнейшего освоения образовательной программы; * с неточностями применяет изученные методы и средства защиты информации при решении поставленных задач; * демонстрирует достаточный уровень программирования и разработки программного обеспечения в области защиты информации; * демонстрирует фрагментарные знания основной учебной литературы по дисциплине; * дает ответы, отражающие знания на базовом уровне теоретического и практического материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профилю обучения. |
| низкий |  | неудовлетворительно | Обучающийся:   * демонстрирует фрагментарные знания теоретического и практического материала, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации; * испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами; * не способен применять изученные методы и средства защиты информации при решении поставленных задач; * не способен программировать и разрабатывать программное обеспечение в области защиты информации; * дает ответы, отражающие отсутствие знаний на базовом уровне теоретического и практического материала в объеме, необходимом для дальнейшей учебы. |

# ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ, ВКЛЮЧАЯ САМОСТОЯТЕЛЬНУЮ РАБОТУ ОБУЧАЮЩИХСЯ

При проведении контроля самостоятельной работы обучающихся, текущего контроля и промежуточной аттестации по учебной дисциплине «Методы криптографической защиты информации» проверяется уровень сформированности у обучающихся компетенций и запланированных результатов обучения по дисциплине*,* указанных в разделе 2 настоящей программы.

## Формы текущего контроля успеваемости, примеры типовых заданий:

| **№ пп** | **Формы текущего контроля** | * + - 1. **Примеры типовых заданий** |
| --- | --- | --- |
| Раздел I | Самостоятельные проверочные работы | 1. Напишите программу, выводящую все простые числа, которые меньше m. 2. Выведите на экран приведенную систему вычетов по модулю m. 3. Напишите функцию, вычисляющую значение φ(m), где φ(m)-функция Эйлера. 4. Напишите программу, представляющую число m в каноническом разложении по степеням простых чисел. 5. Реализуйте расширенный алгоритм Евклида. 6. Реализуйте алгоритм быстрого возведения в степень в кольце вычетов. 7. Напишите программу, представляющую элемент из GF(256) в полиномиальной форме. |
| Раздел II | Самостоятельные проверочные работы | 1. Реализуйте алгоритм RSA. 2. Разработайте приложение, обеспечивающее безопасность данных на основе алгоритма Rijndael. Реализовать возможность выбора длины блока шифротекста и длины ключа. 3. Написать программу, взламывающую шифр Цезаря. 4. Реализовать алгоритм RC4. 5. Написать программу взламывающую шифр, основанный на простом 6. «xor». 7. Реализуйте алгоритм DES. |

## Критерии, шкалы оценивания текущего контроля успеваемости:

| **Наименование оценочного средства (контрольно-оценочного мероприятия)** | **Критерии оценивания** | **Шкалы оценивания** | |
| --- | --- | --- | --- |
| **100-балльная система** | **Пятибалльная система** |
| Самостоятельные проверочные работы | Обучающийся демонстрирует грамотное выполнение всех заданий, использование правильных методов решения при незначительных вычислительных погрешностях; |  | 5 |
| Продемонстрировано использование правильных методов при выполнении заданий, при этом обнаружено наличие существенных ошибок в 1-2 из них; |  | 4 |
| Обучающийся использует верные методы решения, но правильные ответы в большинстве случаев отсутствуют; |  | 3 |
| Обучающимся использованы неверные методы решения, отсутствуют верные ответы. |  | 2 |

## Промежуточная аттестация:

|  |  |
| --- | --- |
| **Форма промежуточной аттестации** | **Типовые контрольные задания и иные материалы**  **для проведения промежуточной аттестации:** |
| Экзамен | Билет 1.   1. Трудные задачи, связанные с проблемой факторизации и их взаимосвязь друг с другом. 2. Алгоритм DES. 3. Покажите, что шифрование в системе Эль-Гамаль требует умножений по модулю .   Билет 2.   1. Понятие диффузии, конфузии. Сеть Фейстеля. 2. Теоретико-информационная стойкость. Различные понятия стойкости. Критерий абсолютно стойкой криптосистемы (теорема Шеннона). 3. Пусть в RSA системе пользователи используют открытый ключ и личные ключи . Некоторый пользователь утверждает, что его личный ключ раскрыт, но вместо генерирования нового модуля сравнения, он решает сгенерировать новые открытый и личный ключи. Насколько это безопасно. Ответ обосновать.   Билет 3.   1. Кольцо вычетов по модулю . Алгоритм возведения в степень в кольце вычетов. Функция Эйлера и ее свойства. Теорема Эйлера. Малая теорема Ферма. 2. Режимы сцепления блоков шифротекста. 3. Пусть у абсолютно стойкой криптосистемы мощности множеств открытых текстов, шифротекстов и ключей равны. Докажите, что шифротексты в такой системе распределены равномерно.   Билет 4.   1. Понятие энтропии и ее свойства. Лемма об энтропии для ключей и шифротекстов. Понятие избыточности языка. Расстояние единственности шифра. 2. Алгоритм RSA. 3. Показать, что в DES первые 24 бита каждого подключа выбираются из одного 28 битного подмножества битов исходного ключа, а вторые 24 бита – из другого, не пересекающегося с первым 28 битным подмножеством битов этого ключа.   Билет 5.   1. Криптосистема Эль-Гамаль. Криптосистема Рабина. 2. Распределение ключей шифрования. Проблемы управления ключами. Схема Шнорра. 3. Пусть поле характеристики . Возможно ли равенство:   ? Ответ обосновать. |

## Критерии, шкалы оценивания промежуточной аттестации учебной дисциплины:

| **Форма промежуточной аттестации** | **Критерии оценивания** | **Шкалы оценивания** | |
| --- | --- | --- | --- |
| **Наименование оценочного средства** | **100-балльная система** | **Пятибалльная система** |
| Экзамен:  в устной форме по билетам | Обучающийся:   * демонстрирует знания, отличающиеся глубиной и содержательностью, дает полный исчерпывающий ответ, как на основные вопросы билета, так и на дополнительные; * свободно выполняет практические задания повышенной сложности, предусмотренные программой, демонстрирует системную работу с основной и дополнительной литературой;   Ответ не содержит фактических ошибок и характеризуется глубиной, полнотой, уверенностью суждений. |  | 5 |
| Обучающийся:   * показывает достаточное знание учебного материала, но допускает несущественные фактические ошибки, которые способен исправить самостоятельно, благодаря наводящему вопросу; * недостаточно раскрыта проблема по одному из вопросов билета; * недостаточно логично построено изложение вопроса; * успешно выполняет предусмотренные в программе практические задания средней сложности, активно работает с основной литературой, * демонстрирует, в целом, системный подход к решению практических задач, к самостоятельному пополнению и обновлению знаний в ходе дальнейшей учебной работы и профессиональной деятельности.   В ответе раскрыто, в основном, содержание билета, имеются неточности при ответе на дополнительные вопросы. |  | 4 |
| Обучающийся:   * показывает знания фрагментарного характера, которые отличаются поверхностностью и малой содержательностью, допускает фактические грубые ошибки; * не может обосновать закономерности и принципы, объяснить факты, нарушена логика изложения, отсутствует осмысленность представляемого материала, представления о межпредметных связях слабые; * справляется с выполнением практических заданий, предусмотренных программой, знаком с основной литературой, рекомендованной программой, допускает погрешности и ошибки при теоретических ответах и в ходе практической работы.   Содержание билета раскрыто слабо, имеются неточности при ответе на основные и дополнительные вопросы билета, ответ носит репродуктивный характер. Неуверенно, с большими затруднениями решает практические задачи или не справляется с ними самостоятельно. |  | 3 |
| Обучающийся, обнаруживает существенные пробелы в знаниях основного учебного материала, допускает принципиальные ошибки в выполнении предусмотренных программой практических заданий. На большую часть дополнительных вопросов по содержанию зачета затрудняется дать ответ или не дает верных ответов. |  | 2 |

## Примерные темы курсовой работы:

* + - * 1. Разработка приложения для шифрования данных с помощью симметричного блочного алгоритма DEAL.
        2. Разработка приложения для шифрования данных с помощью симметричного блочного алгоритма E2.
        3. Разработка приложения для шифрования данных с помощью симметричного блочного алгоритма FROG.
        4. Разработка приложения для шифрования данных с помощью симметричного блочного алгоритма HPC.
        5. Разработка приложения для шифрования данных с помощью симметричного блочного алгоритма RC6.

## Критерии, шкалы оценивания курсовой работы

| **Форма промежуточной аттестации** | **Критерии оценивания** | **Шкалы оценивания** | |
| --- | --- | --- | --- |
| **100-балльная система** | **Пятибалльная система** |
| защита  курсовой работы | * работа выполнена самостоятельно, написанная в рамках задания курсовой работы программа выполнена корректно и запускается без возникновений ошибок; * собран, обобщен и проанализирован достаточный объем литературных источников; * при написании и защите работы продемонстрированы: высокий уровень сформированности профессиональной компетенции, теоретические знания и наличие практических навыков программирования; * работа правильно оформлена и своевременно представлена на кафедру, полностью соответствует требованиям, предъявляемым к содержанию и оформлению курсовых работ;   ответы на вопросы профессиональные, грамотные и исчерпывающие. |  | 5 |
| * тема работы раскрыта, однако написанная программа выполнена с некоторыми неточностями; * собран, обобщен и проанализирован необходимый объем профессиональной литературы, но не по всем аспектам исследуемой темы сделаны выводы и обоснованы практические рекомендации; * при написании и защите работы продемонстрирован: средний уровень сформированности профессиональной компетенции, наличие теоретических знаний и достаточных практических навыков; * работа своевременно представлена на кафедру, есть отдельные недостатки в ее оформлении; * в процессе защиты работы были даны неполные ответы на вопросы. |  | 4 |
| * тема работы раскрыта частично, но в основном правильно, допущены некоторые ошибки при написании программы; * в работе недостаточно полно была использована профессиональная литература, выводы и практические рекомендации не отражали в достаточной степени содержание работы; * при написании и защите работы продемонстрирован удовлетворительный уровень профессиональной компетенции, поверхностный уровень теоретических знаний и практических навыков; * работа своевременно представлена на кафедру, однако не в полном объеме по содержанию и / или оформлению соответствует предъявляемым требованиям; * в процессе защиты недостаточно полно изложены основные положения работы, ответы на вопросы даны неполные. |  | 3 |
| * содержание работы не раскрывает тему, написанная в рамках задания курсовой работы программа выполнена некорректно, работа не оригинальна; * при написании и защите работы продемонстрирован неудовлетворительный уровень компетенции; * работа несвоевременно представлена на кафедру, не в полном объеме по содержанию и оформлению соответствует предъявляемым требованиям; * на защите показаны поверхностные знания по исследуемой теме, отсутствие представлений об актуальных проблемах по теме работы, даны неверные ответы на вопросы. |  | 2 |

## Система оценивания результатов текущего контроля и промежуточной аттестации.

Оценка по дисциплине выставляется обучающемуся с учётом результатов текущей и промежуточной аттестации.

|  |  |  |
| --- | --- | --- |
| **Форма контроля** | **100-балльная система** | **Пятибалльная система** |
| Текущий контроль: |  |  |
| Самостоятельные проверочные работы |  | 2 – 5 |
| Выполнение курсовой работы |  | отлично  хорошо  удовлетворительно  неудовлетворительно |
| Промежуточная аттестация  (экзамен) |  |
| **Итого за семестр** (дисциплину)  экзамен |  |

# ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

* + - 1. Реализация программы предусматривает использование в процессе обучения следующих образовательных технологий:
    - поиск и обработка информации с использованием сети Интернет;
    - дистанционные образовательные технологии в случае производственной необходимости;
    - применение электронного обучения в случае производственной необходимости.

# ПРАКТИЧЕСКАЯ ПОДГОТОВКА

* + - 1. Практическая подготовка в рамках учебной дисциплины реализуется при проведении практических занятий.

# ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

* + - 1. При обучении лиц с ограниченными возможностями здоровья и инвалидовиспользуются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуального обучения, применение соответствующих методик по работе с инвалидами, использование средств дистанционного общения, проведение дополнительных индивидуальных консультаций по изучаемым теоретическим вопросам и практическим занятиям, оказание помощи при подготовке к промежуточной аттестации.
      2. При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса лицам с ограниченными возможностями здоровья, в том числе для дистанционного обучения.
      3. Учебные и контрольно-измерительные материалы представляются в формах, доступных для изучения студентами с особыми образовательными потребностями с учетом нозологических групп инвалидов.
      4. Для подготовки к ответу на практическом занятии, студентам с ограниченными возможностями здоровья среднее время увеличивается по сравнению со средним временем подготовки обычного студента.
      5. Для студентов с инвалидностью или с ограниченными возможностями здоровья форма проведения текущей и промежуточной аттестации устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.).
      6. Промежуточная аттестация по дисциплине может проводиться в несколько этапов в форме рубежного контроля по завершению изучения отдельных тем дисциплины. При необходимости студенту предоставляется дополнительное время для подготовки ответа на зачете или экзамене.
      7. Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации, обучающихся создаются, при необходимости, фонды оценочных средств, адаптированные для лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе.

# МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

* + - 1. Материально-техническое обеспечение дисциплины при обучении с использованием традиционных технологий обучения.

| **Наименование учебных аудиторий, лабораторий, мастерских, библиотек, спортзалов, помещений для хранения и профилактического обслуживания учебного оборудования и т.п.** | **Оснащенность учебных аудиторий, лабораторий, мастерских, библиотек, спортивных залов, помещений для хранения и профилактического обслуживания учебного оборудования и т.п.** |
| --- | --- |
| **119071, г. Москва, Малая Калужская улица, дом 1** | |
| аудитории для проведения занятий лекционного типа | комплект учебной мебели,  технические средства обучения, служащие для представления учебной информации большой аудитории:   * ноутбук; * проектор; * проекционный экран. |
| аудитории для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации | комплект учебной мебели,  технические средства обучения, служащие для представления учебной информации большой аудитории:   * ноутбук; * проектор; * проекционный экран; * персональные компьютеры для обучающихся. |
| **Помещения для самостоятельной работы обучающихся** | **Оснащенность помещений для самостоятельной работы обучающихся** |
| читальный зал библиотеки | * компьютерная техника;   подключение к сети Интернет. |

# УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Автор(ы)** | **Наименование издания** | **Вид издания (учебник, УП, МП и др.)** | **Издательство** | **Год**  **издания** | **Адрес сайта ЭБС**  **или электронного ресурса** | **Количество экземпляров в библиотеке Университета** |
| 10.1 Основная литература, в том числе электронные издания | | | | | | | |
| 1 | Сычев Ю. Н. | Защита информации и информационная безопасность | Учебное пособие | М.: НИЦ ИНФРА-М | 2021 | <https://znanium.com/catalog/product/1844364> | - |
| 2 | Крамаров С. О., Тищенко Е. Н., Соколов С. В., Шевчук П. С., Митясова О. Ю. | Криптографическая защита информации | Учебное пособие | М.: РИОР, ИНФРА-М | 2021 | <https://znanium.com/catalog/product/1153156> | - |
| 3 | Бабаш А. В. | Криптографические методы защиты информации | Учебно-методическое пособие | М.: РИОР, ИНФРА-М | 2018 | <https://znanium.com/catalog/product/960001> | - |
| 10.2 Дополнительная литература, в том числе электронные издания | | | | | | | |
| 1 | Шаньгин В. Ф | Комплексная защита информации в корпоративных системах | Учебное пособие | М.: ФОРУМ, ИНФРА-М | 2020 | <https://znanium.com/catalog/product/1093695> | - |
| 2 | Клименко И. С. | Информационная безопасность и защита информации: модели и методы управления | Учебное пособие | М.: ИНФРА-М | 2020 | <https://znanium.com/catalog/product/1018665> | - |
| 3 | Баранова Е. К. | Информационная безопасность и защита информации | Учебное пособие | М.: РИОР, ИНФРА-М | 2021 | <https://znanium.com/catalog/product/1189326> | - |

# ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА

## Ресурсы электронной библиотеки, информационно-справочные системы и профессиональные базы данных:

|  |  |
| --- | --- |
| **№ пп** | **Электронные учебные издания, электронные образовательные ресурсы** |
|  | ЭБС «Лань» <http://www.e.lanbook.com/> |
|  | «Znanium.com» научно-издательского центра «Инфра-М»  <http://znanium.com/> |
|  | Электронные издания «РГУ им. А.Н. Косыгина» на платформе ЭБС «Znanium.com» <http://znanium.com/> |
|  | Образовательная платформа «Юрайт» <https://urait.ru/> |
|  | Электронные ресурсы «Polpred.com Обзор СМИ» <https://www.polpred.com/> |
|  | Электронные ресурсы «Национальной электронной библиотеки» («НЭБ») <https://rusneb.ru/> |
|  | **Профессиональные базы данных, информационные справочные системы** |
|  | Информационно-аналитическая система SCIENCE INDEX (включенная в научный информационный ресурс eLIBRARY.RU) <https://www.elibrary.ru/> |
|  | База данных Springer eBooks Collections издательства Springer Nature.  Платформа Springer Link: <https://rd.springer.com/> |
|  | Электронный ресурс Freedom Collection издательства Elsevier <https://sciencedirect.com/> |
|  | База данных научного цитирования Scopus издательства Elsevier <https://www.scopus.com/> |
|  | База данных ORBIT IPBI (Platinum Edition) компании Questel SAS <https://www.orbit.com/> |
|  | База данных Web of Science компании Clarivate Analytics <https://www.webofscience.com/wos/woscc/basic-search> |
|  | База данных CSD-Enterprise компании The Cambridge Crystallographic Data Center  <https://www.ccdc.cam.ac.uk/> |
|  | Научная электронная библиотека «elibrary.ru» <https://www.elibrary.ru/> |
|  | База данных издательства SpringerNature  <https://link.springer.com/>  <https://www.springerprotocols.com/>  <https://materials.springer.com/>  [https://link.springer.com/search?facet-content-type=%ReferenceWork%22](https://link.springer.com/search?facet-content-type=%25ReferenceWork%22)  <http://zbmath.org/>  <http://npg.com/> |

## Перечень программного обеспечения

|  |  |  |
| --- | --- | --- |
| **№п/п** | **Программное обеспечение** | **Реквизиты подтверждающего документа/ Свободно распространяемое** |
|  | Windows 10 Pro, MS Office 2019 | контракт № 18-ЭА-44-19 от 20.05.2019 |
|  | Microsoft Visual Studio | контракт № 18-ЭА-44-19 от 20.05.2019 |
|  | PyCharm Community Edition | свободно распространяемое |

### ЛИСТ УЧЕТА ОБНОВЛЕНИЙ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

В рабочую программу учебной дисциплины внесены изменения/обновления и утверждены на заседании кафедры:

|  |  |  |  |
| --- | --- | --- | --- |
| **№ пп** | **год обновления РПД** | **характер изменений/обновлений**  **с указанием раздела** | **номер протокола и дата заседания**  **кафедры** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |