



Федеральное государственное бюджетное образовательное учреждение  
высшего образования

САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ  
АРХИТЕКТУРНО-СТРОИТЕЛЬНЫЙ УНИВЕРСИТЕТ

Кафедра Информационных систем и технологий

УТВЕРЖДАЮ  
Начальник учебно-методического управления

«31» октября 2024 г.

## **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

Защита информации

направление подготовки/специальность 38.03.05 Бизнес-информатика

направленность (профиль)/специализация образовательной программы Бизнес-аналитика

Форма обучения очная

Санкт-Петербург, 2024

## 1. Цели и задачи освоения дисциплины (модуля)

Цель освоения дисциплины:

формирование знаний, умений и навыков использования в профессиональной деятельности методов и алгоритмов защиты информации при хранении информации, передаче по каналам связи, обеспечении безопасности информационных систем.

Задачи освоения дисциплины:

- овладение методами теоретических и экспериментальных исследований в области информационной безопасности;
- получение знаний о современных информационно-коммуникационных технологиях, об инструментальных средах, о программно-технических платформах для решения профессиональных задач с учетом требований ИБ и защиты информации;
- овладение методами практического применения методов и средств обеспечения информационной безопасности при проектировании информационных систем;
- понимать, разрабатывать и аргументировано применять методы обеспечения целостности, конфиденциальности и доступности данных в информационных системах.

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

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, обеспечивающие достижение планируемых результатов освоения ОПОП
ОПК-3 Способен управлять процессами создания и использования продуктов и услуг в сфере информационно-коммуникационных технологий, в том числе разрабатывать алгоритмы и программы для их практической реализации	ОПК-3.1 Осуществляет управление процессами разработки и использования продуктов и услуг в сфере информационно-коммуникационных технологий	<b>знает</b> основные понятия и определения в сфере ИБ и ЗИ, угрозы информационной безопасности, нормативно-правовую базу в сфере ИБ и ЗИ, методы и алгоритмы, в том числе криптографические, защиты информации используемые в практике применения информационно-коммуникационных технологий при решении задач управления процессами разработки и использования продуктов и услуг в сфере ИКТ, защиты информационных ресурсов и баз данных <b>умеет</b> применять знания в сфере ИБ и ЗИ, угроз информационной безопасности, нормативно-правовой базы в сфере ИБ и ЗИ, методов и алгоритмов, в том числе криптографических, защиты информации используемых в практике применения информационно-коммуникационных технологий для решения задач выбора информационных ресурсов в соответствии с поставленной задачей, решения задач защиты информационных ресурсов и баз данных <b>владеет</b> навыками применения знаний в сфере ИБ и ЗИ, угроз информационной безопасности, нормативно-правовой базы в сфере ИБ и ЗИ, методов и алгоритмов, в том числе криптографических, защиты информации используемых в практике применения информационно-коммуникационных технологий для решения задач выбора

		информационных ресурсов в соответствии с поставленной задачей, решения задач защиты информационных ресурсов и баз данных
ОПК-3 Способен управлять процессами создания и использования продуктов и услуг в сфере информационно-коммуникационных технологий, в том числе разрабатывать алгоритмы и программы для их практической реализации	ОПК-3.3 Разрабатывает алгоритмы и программный код для практического применения в информационных системах управления бизнесом	<p><b>знает</b> Методы и алгоритмы, в том числе криптографические, защиты информации используемые в практике применения информационно-коммуникационных технологий в информационных системах управления бизнесом</p> <p><b>умеет</b> применять методы и алгоритмы, в том числе криптографические, для решения задач защиты информации в практике применения информационно-коммуникационных технологий в информационных системах управления бизнесом</p> <p><b>владеет</b> навыками применения методов и алгоритмов, в том числе криптографических, для решения задач защиты информации в практике применения информационно-коммуникационных технологий в информационных системах управления бизнесом</p>
ОПК-5 Способен организовывать взаимодействие с клиентами и партнерами в процессе решения задач управления жизненным циклом информационных систем и информационно-коммуникационных технологий	ОПК-5.1 Применяет основы системного администрирования, системы управления базами данных, информационно-коммуникационные технологии, современные стандарты информационного взаимодействия в процессе создания информационных систем и управления их жизненным циклом с учетом требований информационной безопасности	<p><b>знает</b> нормативную базу в сфере защиты информации, способы системного администрирования, современные ИКТ технологии защиты информации, применяемые в процессе создания информационных систем и управления их жизненным циклом с учетом требований информационной безопасности</p> <p><b>умеет</b> применять нормативную базу в сфере защиты информации, способы системного администрирования, современные ИКТ технологии защиты информации при решении практических задач создания информационных систем и/или управления их жизненным циклом с учетом требований информационной безопасности</p> <p><b>владеет</b> навыками применения нормативной базы в сфере защиты информации, способов системного администрирования, современных ИКТ технологий защиты информации при решении практических задач создания информационных систем и/или управления их жизненным циклом с учетом требований информационной безопасности</p>

### 3. Указание места дисциплины (модуля) в структуре образовательной программы

Данная дисциплина (модуль) включена в Блок «Дисциплины, модули» Б1.О.28 основной профессиональной образовательной программы 38.03.05 Бизнес-информатика и относится к обязательной части учебного плана.

№ п/п	Предшествующие дисциплины	Код и наименование индикатора достижения компетенции
1	Информационные технологии	УК-1.1, УК-1.2, УК-1.6, ОПК-4.1, ОПК-4.2, ОПК-4.3
2	ИТ- инфраструктура предприятия	ОПК-1.1, ОПК-1.2, ОПК-1.3, ОПК-2.1, ОПК-5.1
3	Основы программирования	ОПК-3.1, ОПК-3.2, ОПК-3.3

Для успешного освоения дисциплины обучающемуся необходимо:

знать:

- общие принципы функционирования вычислительных систем;
- общие принципы построения вычислительных алгоритмов;
- язык программирования;
- средства компьютерного моделирования и программирования;

уметь:

- проводить разработку алгоритмов на основе современного математического аппарата и информационных технологий;

- программировать алгоритм, используя средства языка высокого уровня;

владеть:

- основными приёмами работы на компьютерах с прикладным программным обеспечением;
- разрабатывать прикладные программы, используя язык программирования и средства компьютерного моделирования.

№ п/п	Последующие дисциплины	Код и наименование индикатора достижения компетенции
1	Проектная практика	ПК-1.1, ПК-1.2, ПК-2.1, ПК-2.3, ПК-2.4, ПК-3.1, ПК-3.2, ПК-3.3, ПК-4.1, ПК-4.2, ПК-5.1, ПК-5.3
2	Управление ИТ-проектами и безопасность бизнес-процессов	ПК-4.1, ПК-4.2, ПК-4.3

**4. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся**

Вид учебной работы	Всего часов	Из них часы на практическую подготовку	Семестр
			6
<b>Контактная работа</b>	48		48
Лекционные занятия (Лек)	16	0	16
Практические занятия (Пр)	32	0	32
<b>Иная контактная работа, в том числе:</b>	0,25		0,25
консультации по курсовой работе (проекту), контрольным работам (РГР)			
контактная работа на аттестацию (сдача зачета, зачета с оценкой; защита курсовой работы (проекта); сдача контрольных работ (РГР))			
контактная работа на аттестацию в сессию (консультация перед экзаменом и сдача	0,25		0,25
<b>Часы на контроль</b>	8,75		8,75
<b>Самостоятельная работа (СР)</b>	51		51
<b>Общая трудоемкость дисциплины (модуля)</b>			
<b>часы:</b>	108		108
<b>зачетные единицы:</b>	3		3



5.1.	Зачет с оценкой	6							9	ОПК-3.1, ОПК-3.3, ОПК-5.1
------	-----------------	---	--	--	--	--	--	--	---	---------------------------------

### 5.1. Лекции

№ разд	Наименование раздела и темы лекций	Наименование и краткое содержание лекций
1	Основы информационной безопасности и защиты информации	<p>Основы информационной безопасности</p> <p>Основные понятия и определения в области информационной безопасности</p> <p>Обеспечение свойства информации: конфиденциальности, целостности, доступности.</p> <p>Основные понятия и определения, относящиеся к ИБ. Необходимость защиты информации. Основные задачи обеспечения защиты информации. Объекты, цели и задачи защиты информации</p> <p>Угрозы информационной безопасности. Каналы утечки информации</p> <p>Понятие угрозы. Классификация видов угроз ИБ по различным признакам. Угрозы доступности, целостности и конфиденциальности.</p> <p>Классификация атак. Сетевые атаки. Окно опасности.</p>
2	Классы ИБ. Программно-технический уровень ИБ	<p>Классы ИБ. Программно-технический уровень защиты информации</p> <p>Критерии безопасности компьютерных систем ("Оранжевая книга").</p> <p>Классы, уровни защищенности компьютерных систем. Политики безопасности</p> <p>Основные понятия программно-технического уровня ИБ.</p> <p>Архитектурная безопасность. Парольная аутентификация.</p> <p>Одноразовые пароли. Идентификация/ аутентификация с помощью биометрических данных. Протоколирование. Активный аудит.</p> <p>Функциональные компоненты и архитектура. Криптография.</p> <p>Стеганография. Управление доступом.</p>
4	Симметричные системы шифрования	<p>Симметричные системы шифрования</p> <p>Простейшие системы шифрования (шифр замены, перестановки, шифры Вернама, Вижинера, гаммирование). Современные симметричные криптосистемы. Блочные и поточные шифры.</p> <p>Гаммирование. Шифр DES, режимы работы DES, AES, ГОСТ 28147-89.</p>
5	Асимметричные системы шифрования	<p>Асимметричные системы шифрования</p> <p>Общая схема функционирования систем с открытыми ключами, основанными на односторонних функциях. Криптосистема RSA и ее модификации. Криптосистема Эль Гамала (El Gamal).</p>
6	Криптографические протоколы. Управление ключами	<p>Криптографические протоколы. Управление ключами</p> <p>Характеристика протоколов идентификации и аутентификации, идентификация на основе пароля. Взаимная проверка подлинности пользователей. Протоколы с нулевой передачей знаний (Шнорра, Фейджа-Фиата-Шамира). Схемы обязательств. Распределение ключей</p> <p>Выбор ключа, время жизни ключа, разделение секрета.</p> <p>Схемы обмена секретными ключами: Шамира, Диффи-Хеллмана.</p> <p>Схемы разделения секрета</p>
7	Электронная цифровая подпись	<p>Электронная цифровая подпись</p> <p>Целостность данных и аутентификация сообщений. Хэш-функции (MD4, SHA). Алгоритмы ЭЦП, основанные на односторонних функциях: RSA, Эль Гамала, DSA, Шнорра</p>
8	Цифровые сертификаты и	<p>Цифровые сертификаты и инфраструктура открытых ключей</p> <p>Системы перераспределения доверия: PGP, SSL, X509 (PKIX), SPKI.</p>

	инфраструктура открытых ключей	Неявные сертификаты.
9	Правовое обеспечение информационной безопасности	Правовое обеспечение информационной безопасности Структура государственной системы информационной безопасности. Органы (подразделения), обеспечивающие информационную безопасность. Федеральные законы, регламентирующие ИБ и ЗИ: Об информации, информационных технологиях и о защите информации; О персональных данных; О коммерческой тайне; Об электронной подписи; О безопасности критической информационной инфраструктуры РФ

## 5.2. Практические занятия

№ разд	Наименование раздела и темы практических занятий	Наименование и содержание практических занятий
1	Основы информационной безопасности и защиты информации	Основы информационной безопасности Защита информации в пакетах офисных программ. Освоение средств защиты информации, доступных в пакетах офисных программ (текстовый редактор, табличный процессор).
2	Классы ИБ. Программно-технический уровень ИБ	Программно-технический уровень защиты информации Политика безопасности операционной системы Изучение и настройка локальных политик безопасности на уровне операционной системы
3	Элементы теории чисел	Элементы теории чисел Функция Эйлера. Сравнения. Сравнимые по модулю $m$ числа. Сравнения, свойства сравнений, вычеты, полная система вычетов, приведенная система вычетов, теоремы Эйлера и Ферма. Символ Лежанда, Якоби. Квадратичные вычеты. Сравнения первой степени с одним неизвестным. Система сравнений первой степени. Китайская теорема об остатках. Сравнения любой степени по простому и составному модулю. Сравнения второй степени. Моноиды, группы, кольца, идеалы, поля, полиномиальные кольца над полями, полиномиальные коды, регистры сдвига. Примитивные элементы, базисы, представления конечных полей, первообразные корни, индексы и дискретные логарифмы. Кодовые последовательности. Блочные коды и их свойства. Криптографические хэш-функции Эллиптические кривые и их свойства.
4	Симметричные системы шифрования	Потоковые системы шифрования Рекуррентные последовательности. Характеристические функции кодовых последовательностей. Примитивные многочлены, неприводимые многочлены и их построение. Поточные шифры: РСЛОС, RC4
5	Асимметричные системы шифрования	Асимметричные системы шифрования Асимметричные криптосистемы. Реализация алгоритмов RSA, El-Gamal. Реализация алгоритмов на языках программирования и/или в математических пакетах прикладных программ (Maple, Matlab, Python, PyCharm Community)
6	Криптографические протоколы. Управление ключами	Криптографические протоколы. Управление ключами Схемы обмена секретными ключами: Шамира, Диффи-Хеллмана. Протоколы с нулевой передачей знаний. Схемы разделения секрета. Реализация алгоритмов на языках программирования и/или в



		математических пакетах прикладных программ (Maple, Matlab, Python, PyCharm Community)
7	Электронная цифровая подпись	Электронная цифровая подпись Алгоритмы ЭЦП, основанные на односторонних функциях: RSA, Эль Гамала. Реализация алгоритмов на языках программирования и/или в математических пакетах прикладных программ (Maple, Matlab, Python, PyCharm Community)
9	Правовое обеспечение информационной безопасности	Правовое обеспечение информационной безопасности Структура государственной системы информационной безопасности. Органы (подразделения), обеспечивающие информационную безопасность. Федеральные законы, регламентирующие ИБ и ЗИ: Об информации, информационных технологиях и о защите информации; О персональных данных; О коммерческой тайне; Об электронной подписи; О безопасности критической информационной инфраструктуры РФ

### 5.3. Самостоятельная работа обучающихся

№ разд	Наименование раздела дисциплины и темы	Содержание самостоятельной работы
1	Основы информационной безопасности и защиты информации	Основы информационной безопасности Изучение теоретического материала, подготовка к устным опросам, выполнение практических заданий
2	Классы ИБ. Программно-технический уровень ИБ	Классы ИБ. Программно-технический уровень защиты информации Изучение теоретического материала, подготовка к устным опросам, выполнение практических заданий
3	Элементы теории чисел	Элементы теории чисел Изучение теоретического материала, подготовка к устным опросам, выполнение практических заданий
4	Симметричные системы шифрования	Симметричные системы шифрования Изучение теоретического материала, подготовка к устным опросам
5	Асимметричные системы шифрования	Асимметричные системы шифрования Изучение теоретического материала, подготовка к устным опросам, выполнение практических заданий
6	Криптографические протоколы. Управление ключами	Криптографические протоколы. Управление ключами Изучение теоретического материала, подготовка к опросам, практические задания
7	Электронная цифровая подпись	Электронная цифровая подпись Изучение теоретического материала, подготовка к опросам, практические задания
8	Цифровые сертификаты и инфраструктура открытых ключей	Цифровые сертификаты и инфраструктура открытых ключей Изучение теоретического материала, подготовка к опросам
9	Правовое обеспечение информационной безопасности	Правовое обеспечение информационной безопасности Изучение теоретического материала, подготовка к опросам, практические задания

## 6. Методические материалы для самостоятельной работы обучающихся по дисциплине (модулю)

### 1. Методические рекомендации по изучению дисциплины

Студентам необходимо ознакомиться: - с содержанием рабочей программы дисциплины (далее - РПД), с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, методическими разработками по данной дисциплине, имеющимся на образовательном портале и сайте кафедры, с графиком консультаций преподавателей кафедры.

Самостоятельная работа студентов включает в себя выполнение различного рода заданий, которые ориентированы на более глубокое усвоение материала изучаемой дисциплины. По каждой теме учебной дисциплины студентам предлагается перечень заданий для самостоятельной работы. К выполнению заданий для самостоятельной работы предъявляются следующие требования: задания должны исполняться самостоятельно и представляться в установленный срок, а также соответствовать установленным требованиям по оформлению.

Студентам следует:

- выполнять все плановые задания, выдаваемые преподавателем для самостоятельного выполнения, и разбирать на практических занятиях и консультациях неясные вопросы;
- использовать при подготовке нормативные документы университета;
- при подготовке к зачету с оценкой прорабатывать соответствующие теоретические и практические разделы дисциплины, фиксируя неясные моменты для их обсуждения на консультации.

### 2. Рекомендации по подготовке к лекционным занятиям (теоретический курс)

Изучение дисциплины требует систематического и последовательного накопления знаний, следовательно, пропуски отдельных тем не позволяют глубоко освоить предмет. Именно поэтому контроль над систематической работой студентов всегда находится в центре внимания кафедры. Студентам необходимо:

- на отдельные лекции иметь при себе на бумажных или электронных носителях рекомендуемый лектором материал по соответствующим темам из разделов основных и дополнительных источников литературы или переданный лектором в электронном виде (таблицы, графики, схемы, презентации и т.п.). Данный материал будет охарактеризован, прокомментирован, дополнен непосредственно на лекции;
- перед очередной лекцией необходимо просмотреть по конспекту материал предыдущих лекций. При затруднениях в восприятии материала следует обратиться к основным и(или) дополнительным литературным источникам. Если разобраться в материале опять не удалось, то необходимо обратиться к лектору (по графику его консультаций) или к преподавателю на практических занятиях. Не оставляйте «белых пятен» в освоении материала.

Студентам, пропустившим занятия (независимо от причин), рекомендуется переписать конспект пропущенной лекции, проработать материал по литературным источникам, при возникновении вопросов по пропущенной теме явиться на консультацию к преподавателю и задать интересующие вопросы по теме пропущенного занятия.

### 3. Рекомендации по подготовке к практическим занятиям

Студентам следует:

- приносить с собой рекомендованную преподавателем литературу (таблицы, графики, схемы, презентации и т.п.) к конкретному занятию;
- до очередного практического занятия по рекомендованным литературным источникам проработать теоретический материал, соответствующей темы занятия;
- в начале занятий задать преподавателю вопросы по материалу, вызвавшему затруднения в его понимании и освоении при решении задач, заданных для самостоятельного решения;
- в ходе практического занятия давать конкретные, четкие ответы по существу вопросов;
- на занятии доводить каждую задачу до окончательного решения, демонстрировать понимание проведенных расчетов (анализов, ситуаций), в случае затруднений обращаться к преподавателю.

## 7. Оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине (модулю)

### 7.1. Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины

№ п/п	Контролируемые разделы дисциплины (модуля)	Код и наименование индикатора контролируемой компетенции	Вид оценочного средства
1	Основы информационной безопасности и защиты информации	ОПК-3.1, ОПК-5.1	Вопросы для опросов, практические задания
2	Классы ИБ. Программно-технический уровень ИБ	ОПК-3.1	Вопросы для опросов, практические задания
3	Элементы теории чисел	ОПК-3.3	Вопросы для опросов, практические задания
4	Симметричные системы шифрования	ОПК-3.3	Вопросы для опросов, практические задания
5	Асимметричные системы шифрования	ОПК-3.1, ОПК-3.3, ОПК-5.1	Вопросы для опросов, практические задания
6	Криптографические протоколы. Управление ключами	ОПК-3.1, ОПК-3.3, ОПК-5.1	Вопросы для опросов, практические задания
7	Электронная цифровая подпись	ОПК-3.1, ОПК-3.3, ОПК-5.1	Вопросы для опросов, практические задания
8	Цифровые сертификаты и инфраструктура открытых ключей	ОПК-3.1, ОПК-3.3, ОПК-5.1	Вопросы для опросов, практические задания
9	Правовое обеспечение информационной безопасности	ОПК-3.1, ОПК-5.1	Вопросы для опросов, практические задания
10	Зачет с оценкой	ОПК-3.1, ОПК-3.3, ОПК-5.1	Вопросы для промежуточной аттестации, практические задания для промежуточной аттестации

7.2. Типовые контрольные задания или иные материалы текущего контроля успеваемости, необходимые для оценки знаний, умений и навыков и (или) опыта профессиональной деятельности, характеризующих этапы формирования компетенций в процессе освоения дисциплины

Задания для проверки сформированности достижения компетенций ОПК-3.1, ОПК-3.3, ОПК-5.1

Задание 1. Освоить средства защиты информации, доступные в пакетах офисных программ: Функции защиты информации от случайных изменений в текстовых редакторах, табличных процессорах

Ответить на вопросы: Какие задачи защиты информации решают рассмотренные функции приложений офисных пакетов? На какие группы эти функции можно разделить? Почему при открытии файла, сохранённого с двумя паролями, нельзя ввести сразу второй пароль (пароль на редактирование) и сразу открыть документ с возможностью внесения изменений? Влияет ли на доступ к документу значение флажка «Открыть только для чтения»? Если да, то в каких случаях? Проверьте и свои предположения. Как можно защитить часть текста в документе Libre Office Writer? Какие изменения в интерфейсе рассмотренных программ происходят при установке курсора в область, защищённую от изменений? Как реагируют приложения из офисного пакета на попытку изменить содержимое защищённой части документа? Какие функции защиты информации есть в программе Calc? Чем отличается набор функций защиты информации в приложениях Calc и Writer?

Задание 2. Освоить инструментарий настройки политики безопасности установленной операционной системы. Изучить раздел «Администрирование»; изучить «Брандмауэр» и «Защитник»; Изучить элементы управления учетными записями установленной операционной

системы;

Выполнить задания:

№ 1 Открыть «Локальная политика безопасности» средство «Политика учетных записей» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

№ 2 Открыть «Локальная политика безопасности»—«Локальные политики» средство «Политика аудита» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

№ 3 Открыть «Локальная политика безопасности»—«Локальные политики» средство «Назначение прав пользователей» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

№ 5 Открыть «Локальная политика безопасности» средство «Брандмауэр в режиме повышенной безопасности» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

№ 6 Открыть «Локальная политика безопасности» средство «Политики диспетчера списка сетей» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

№ 7 Открыть «Локальная политика безопасности» средство «Политики открытого ключа» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

№ 8 Открыть «Локальная политика безопасности» средство «Политики ограниченного использования программ» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

№ 9 Открыть «Локальная политика безопасности» средство «Политики управления приложениями» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

№ 10 Открыть «Локальная политика безопасности» средство «Политики IP-безопасности» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

№ 11 Открыть «Локальная политика безопасности» средство «Конфигурации расширенной политики аудита» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности.

№ 12 Открыть средство «Брандмауэр» и изучить его. В отчете перечислить возможные настройки и назначение этого средства безопасности

Задание 3.

1 Используя алгоритм Евклида определить НОД чисел  $\text{НОД}(a,b)$

2 Построить подходящую дробь для  $a/b$

3 Используя алгоритм Эратосфена найти все простые числа не превосходящие  $N$

4 Найти каноническое разложение числа  $a$

5 Вычислить значение функции Эйлера для чисел  $a$  и  $p$

6 Для заданного модуля  $m$  выписать полную систему вычетов, приведенную систему вычетов, систему наибольших по абсолютной величине вычетов

7 Решить сравнение  $c \cdot x = d \pmod{p}$

8 Решить сравнение  $c \cdot 3^x = d \cdot 3 \pmod{p^3}$

9 Решить систему сравнений:  $c_1 \cdot x = d_1 \pmod{p_1}$ ;  $c_2 \cdot x = d_2 \pmod{p_2}$ ;  $c_3 \cdot x = d_3 \pmod{p_3}$

10 Вычислить значения символа Лежандра и . Для символа Лежандра равного 1 решить сравнение

Задание 4

1 Построить кодовые последовательности для заданного разностного уравнения над полем вычетов по модулю  $m=5$ , используя начальные вектора

2 Построить кодовые последовательности для заданного характеристического многочлена над полем вычетов по модулю  $m=5$ : путем деления многочлена на многочлен

3 Реализовать программно поточную систему шифрования на основе разностного кода

Задание 5

Написать программу, реализующую асимметричную систему шифрования. четные варианты: алгоритм RSA; нечетные варианты: алгоритм El-Gamal

Задание 6

1) Разработать программу, реализующую схему обмена ключами, алгоритм Диффи-Хеллмана;

- 2) Разработать программу, реализующую схему обмена ключами, схему Шамира
- 3) Необходимо разделить секрет «К» между 5-ю сторонами. При этом любые 3 стороны должны иметь возможность восстановить этот секрет. Реализовать схему Шамира при модуле P (по вариантам). Показать восстановление секрета. Пример варианта: K=5, P=11
- 4) Построить (3,3) – пороговую схему на основе китайской теоремы об остатках для деления секрета N, пример варианта: N=595

Задание 8

- 1) Реализовать программно алгоритм цифровой подписи El-Gamal
- 2) Реализовать программно алгоритм цифровой подписи RSA

Задание 9

Изучить основные законы в сфере ИБ, ответить на вопросы

9. На основании статей Федерального закона от 06.04.2011 N 63-ФЗ (ред. от 02.07.2013) "Об электронной подписи" (с изм. и доп., вступающими в силу с 01.09.2013), необходимо ответить на вопросы Какие виды ЭЦП существуют в РФ. Составьте классификацию в виде схемы видов электронных подписей, их состава и особенностей.

1. С помощью чего создается простая электронная подпись. Приведите примеры средств простой электронной подписи.

2. В чем особенность усиленной неквалифицированной электронной подписи?

3. В каких случаях применяют простые и усиленные неквалифицированные подписи?

4. Какая подпись может использоваться гражданами для отправки сообщений органам власти

5. Какая подпись может рассматриваться как аналог документа с печатью.

6. Что приравнивается к квалифицированным подписям?

7. Что обязательно должно входить в состав усиленной подписи квалифицированной подписи?

8. С помощью, какой подписи можно организовать юридически значимый электронный документооборот с другими компаниями, органами государственной власти и внебюджетными фондами?

9. Во всех ли случаях усиленная квалифицированная электронная подпись может заменить бумажные документы.

10. Кто в России выдает юридически значимый сертификат?

11. Каковы условия признания электронных документов, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью

12. Каковы условия использования простой электронной подписи?

13. Каковы обязанности участников электронного взаимодействия при использовании усиленных электронных подписей?

14. До каких пор признается действительной квалифицированная электронная подпись? При каких условиях.

15. Какие требования предъявляются к средствам электронной подписи?

16. Какие особенности функционирования удостоверяющего центра в РФ.

17. На основании чего и кто создает и выдает сертификаты ключа для проверки электронной подписи?

18. Какую информацию должен содержать сертификат ключа проверки электронной подписи.

19. Какие существуют особенности выдачи сертификата юридическому лицу?

20. До какого срока действует сертификат проверки ключей?

21. Когда прекращает действие сертификат проверки ключей?

22. В течении какого времени, удостоверяющий центр аннулирует сертификат ключа, и по какому условию?

23. Какую информацию обязан хранить аккредитованный удостоверяющий центр.

24. Как получить аккредитацию удостоверяющему центру: на основании какого финансового обеспечения, в какой срок, какой кадровый состав?

25. В чем отличие по составу квалифицированного сертификата от обычного сертификата?

26. Каковы условия выдачи квалифицированного сертификата?

27. Что станет с сертификатом ключей подписи, выданном до 2011 года?

28. Что становится с электронным документом, подписанным электронной подписью до 2008 года, ключ проверки которой содержится в сертификате ключа проверки электронной подписи?

29. До какого срока может действовать сертификат, выданный в 2010 году, срок действия которого заканчивается 5 мая 2014 года?

Оформить в текстовом редакторе ответом на конкретный вопрос и с ссылкой на соответствующую статью Федерального закона.

### 7.3. Система оценивания результатов обучения по дисциплине (модулю) при проведении текущего контроля успеваемости

Оценка «отлично» (зачтено)	знания: - систематизированные, глубокие и полные знания по всем разделам дисциплины, а также по основным вопросам, выходящим за пределы учебной программы; - точное использование научной терминологии, систематически грамотное и логически правильное изложение ответа на вопросы; - полное и глубокое усвоение основной и дополнительной литературы, рекомендованной рабочей программой по дисциплине (модулю) умения: - умеет ориентироваться в теориях, концепциях и направлениях дисциплины и давать им критическую оценку, используя научные достижения других дисциплин навыки: - высокий уровень сформированности заявленных в рабочей программе компетенций; - владеет навыками самостоятельно и творчески решать сложные проблемы и нестандартные ситуации; - применяет теоретические знания для выбора методики выполнения заданий; - грамотно обосновывает ход решения задач; - безупречно владеет инструментарием учебной дисциплины, умение его эффективно использовать в постановке научных и практических задач; - творческая самостоятельная работа на практических/семинарских/лабораторных занятиях, активно участвует в групповых обсуждениях, высокий уровень культуры исполнения заданий
-------------------------------	---

<p>Оценка «хорошо» (зачтено)</p>	<p>знания: - достаточно полные и систематизированные знания по дисциплине; - усвоение основной и дополнительной литературы, рекомендованной рабочей программой по дисциплине (модулю)</p> <p>умения: - умеет ориентироваться в основных теориях, концепциях и направлениях дисциплины и давать им критическую оценку; - использует научную терминологию, лингвистически и логически правильно излагает ответы на вопросы, умеет делать обоснованные выводы; - владеет инструментарием по дисциплине, умение его использовать в постановке и решении научных и профессиональных задач</p> <p>навыки: - самостоятельная работа на практических занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий; - средний уровень сформированности заявленных в рабочей программе компетенций; - без затруднений выбирает стандартную методику выполнения заданий; - обосновывает ход решения задач без затруднений</p>
<p>Оценка «удовлетворительно» (зачтено)</p>	<p>знания: - достаточный минимальный объем знаний по дисциплине; - усвоение основной литературы, рекомендованной рабочей программой; - использование научной терминологии, стилистическое и логическое изложение ответа на вопросы, умение делать выводы без существенных ошибок</p> <p>умения: - умеет ориентироваться в основных теориях, концепциях и направлениях по дисциплине и давать им оценку; - владеет инструментарием учебной дисциплины, умение его использовать в решении типовых задач; - умеет под руководством преподавателя решать стандартные задачи</p> <p>навыки: - работа под руководством преподавателя на практических занятиях, допустимый уровень культуры исполнения заданий; - достаточный минимальный уровень сформированности заявленных в рабочей программе компетенций; - испытывает затруднения при обосновании алгоритма выполнения заданий</p>
<p>Оценка «неудовлетворительно» (не зачтено)</p>	<p>знания: - фрагментарные знания по дисциплине; - отказ от ответа (выполнения письменной работы); - знание отдельных источников, рекомендованных рабочей программой по дисциплине;</p> <p>умения: - не умеет использовать научную терминологию; - наличие грубых ошибок</p> <p>навыки: - низкий уровень культуры исполнения заданий; - низкий уровень сформированности заявленных в рабочей программе компетенций; - отсутствие навыков самостоятельной работы; - не может обосновать алгоритм выполнения заданий</p>

7.4. Теоретические вопросы и практические задания для проведения промежуточной аттестации обучающихся, необходимые для оценки знаний, умений и навыков и (или) опыта профессиональной деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

#### 7.4.1. Теоретические вопросы для проведения промежуточной аттестации обучающихся

Примерные теоретические вопросы для проведения промежуточной аттестации обучающихся

- Угрозы ИБ
- Приведите основные понятия в сфере ИБ
- Уязвимость (информационной системы)
- Атаки на компьютерную систему
- Политика безопасности
- Приведите классификацию угроз ИБ
- Виды несанкционированного доступа
- Виды Вредоносных программ
- Непрограммные угрозы
- Атака доступа, виды атак доступа
- Атака модификации
- Атаки отказа в обслуживании
- Атаки Посредничество
- Атака эксплойта
- Парольные атаки
- Фишинг, фарминг
- Уязвимости и угрозы беспроводных сетей
- Подходы к обеспечению ИБ
- Меры законодательного уровня
- Меры административно-организационного уровня
- Классы ИБ
- Уровни ИБ
- Программно-технический уровень ИБ
- Система шифрования ГОСТ, режимы функционирования ГОСТ
- Система шифрования DES, режимы функционирования DES
- Блочные шифры
- Понятие асимметричной системы шифрования, односторонние функции
- Шифр RSA, модификации RSA
- Шифр El-Gamal
- Протоколы идентификации и аутентификации
- Протокол Феджа-Фиата-Шамира
- Протокол Шнорра
- Парольная защита, схемы реализации
- Протокол обмена ключами Диффи-Хеллмана
- Протокол обмена ключами Шамира
- Схемы разделения секрета
- Цифровая подпись RSA
- Цифровая подпись El-Gamal
- Цифровая подпись DSA
- Криптографические Хэш-функции
- Потоковые системы шифрования
- Цифровые сертификаты
- Законы в сфере ИБ

#### 7.4.2. Практические задания для проведения промежуточной аттестации обучающихся

1. Зашифровать текст «Небо синее, трава зеленая» используя шифр Вижинера, ключ «море». Расшифровать полученный текст.

5. Вычислить секретный ключ. Зашифровать и расшифровать сообщение  $M$ , используя алгоритм RSA и следующие данные  $M=2$   $P=11$   $Q=17$   $K_0=7$

6. Вычислить секретный ключ. Зашифровать и расшифровать сообщение  $M$ , используя алгоритм RSA и следующие данные  $M=3$   $P=47$   $Q=1$   $K_0=7$

7. Вычислить секретный ключ. Зашифровать и расшифровать сообщение  $M$ , используя алгоритм RSA и следующие данные  $M=3$   $P=29$   $Q=1$   $K_0=9$



8. Вычислить секретный ключ. Зашифровать и расшифровать сообщение  $M$ , используя алгоритм RSA и следующие данные  $M=5$   $P=29$   $Q=3$   $K_0=11$
9. Зашифровать и расшифровать сообщение  $M$ , используя алгоритм Эль Гамала и следующие данные  $M=2$   $P=79$   $G=3$   $x=11$   $K=5$
10. Зашифровать и расшифровать сообщение  $M$ , используя алгоритм Эль Гамала и следующие данные  $M=10$   $P=53$   $G=8$   $x=5$   $K=7$
11. Зашифровать и расшифровать сообщение  $M$ , используя алгоритм Эль Гамала и следующие данные  $M=2$   $P=47$   $G=5$   $x=3$   $K=11$
12. Зашифровать и расшифровать сообщение  $M$ , используя алгоритм Эль Гамала и следующие данные  $M=3$   $P=61$   $G=9$   $x=7$   $K=11$
13. Необходимо разделить секрет «5» между 5-ю сторонами. При этом любые 3 стороны должны иметь возможность восстановить этот секрет. Реализовать схему Шамира. Исходные данные:  $p=11$ ,  $F(x)=(7x^2+3x+5) \bmod 11$ . Показать восстановление секрета.
14. Необходимо разделить секрет «7» между 5-ю сторонами. При этом любые 3 стороны должны иметь возможность восстановить этот секрет. Реализовать схему Шамира. Исходные данные:  $p=17$ ,  $F(x)=(5x^2+3x+7) \bmod 17$ . Показать восстановление секрета.
15. Необходимо разделить секрет «7» между 5-ю сторонами. При этом любые 3 стороны должны иметь возможность восстановить этот секрет. Реализовать схему Шамира. Исходные данные:  $p=13$ ,  $F(x)=(3x^2+11x+7) \bmod 13$ . Показать восстановление секрета.
16. Создать у двух абонентов А и В ключ используя схему Шамира, при следующих параметрах системы  $P=13$ ,  $a=3$ ,  $b=5$ , ключ сеанса выбрать самостоятельно.
17. Создать у двух абонентов А и В ключ используя схему Шамира, при следующих параметрах системы  $P=17$ ,  $a=7$ ,  $b=5$ , ключ сеанса выбрать самостоятельно.
18. Построить (3,3) – пороговую схему на основе китайской теоремы об остатках для разделения секрета  $N=295$
19. Построить (3,3) – пороговую схему на основе китайской теоремы об остатках для разделения секрета  $N=315$
20. Используя алгоритмы ЭЦП RSA, подписать сообщение и сделать проверку. Исходные данные:  $P=3$ ,  $Q=29$ ,  $m=h(M)=7$ ,  $K_0=11$ .
21. Создать у двух абонентов А и В ключ используя схему Шамира, при следующих параметрах системы  $P=13$ ,  $a=7$ ,  $b=5$ , ключ сеанса выбрать самостоятельно.
22. Используя алгоритмы ЭЦП RSA, подписать сообщение и сделать проверку. Исходные данные:  $P=3$ ,  $Q=29$ ,  $m=h(M)=5$ ,  $K_0=7$ .
23. Используя алгоритмы ЭЦП RSA, подписать сообщение и сделать проверку. Исходные данные:  $P=3$ ,  $Q=23$ ,  $m=h(M)=7$ ,  $K_0=11$ .
24. Построить (3,3) – пороговую схему на основе китайской теоремы об остатках для разделения секрета  $N=325$

#### 7.4.3. Примерные темы курсовой работы (проекта) (при наличии)

Курсовая работа по дисциплине не предусмотрена учебным планом

7.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта профессиональной деятельности, характеризующие этапы формирования компетенций

Процедура проведения промежуточной аттестации и текущего контроля успеваемости регламентируется локальным нормативным актом, определяющим порядок организации и проведения текущего контроля успеваемости и промежуточной аттестации обучающихся. Типовые контрольные задания или иные материалы текущего контроля приведены в п. 7.2. Вопросы для промежуточной аттестации приведены в п.п. 7.4.1; задания для промежуточной аттестации в п.п. 7.4.2. Процедура оценивания формирования компетенций при проведении промежуточной аттестации приведена в п. 7.6. Форма аттестации - зачет с оценкой.

7.6. Критерии оценивания сформированности компетенций при проведении промежуточной аттестации

	Уровень освоения и оценка			
	Оценка «неудовлетворительно»	Оценка «удовлетворительно»	Оценка «хорошо»	Оценка «отлично»
	«не зачтено»	«зачтено»		
Критерии оценивания	<p>Уровень освоения компетенции «недостаточный». Компетенции не сформированы. Знания отсутствуют, умения и навыки не сформированы</p>	<p>Уровень освоения компетенции «пороговый». Компетенции сформированы. Сформированы базовые структуры знаний. Умения фрагментарны и носят репродуктивный характер. Демонстрируется низкий уровень самостоятельности практического навыка.</p>	<p>Уровень освоения компетенции «продвинутый». Компетенции сформированы. Знания обширные, системные. Умения носят репродуктивный характер, применяются к решению типовых заданий. Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка.</p>	<p>Уровень освоения компетенции «высокий». Компетенции сформированы. Знания аргументированные, всесторонние. Умения успешно применяются к решению как типовых, так и нестандартных творческих заданий. Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка</p>

<p>знания</p>	<p>Обучающийся демонстрирует: -существенные пробелы в знаниях учебного материала; -допускаются принципиальные ошибки при ответе на основные вопросы билета, отсутствует знание и понимание основных понятий и категорий; -непонимание сущности дополнительных вопросов в рамках заданий билета.</p>	<p>Обучающийся демонстрирует: -знания теоретического материала; -неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; -неуверенные и неточные ответы на дополнительные вопросы.</p>	<p>Обучающийся демонстрирует: -знание и понимание основных вопросов контролируемого объема программного материала; - знания теоретического материала -способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; -правильные и конкретные, без грубых ошибок, ответы на поставленные вопросы.</p>	<p>Обучающийся демонстрирует: -глубокие, всесторонние и аргументированные знания программного материала; -полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий, в рамках обсуждаемых заданий; -способность устанавливать и объяснять связь практики и теории, -логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора.</p>
<p>умения</p>	<p>При выполнении практического задания билета обучающийся продемонстрировал недостаточный уровень умений. Практические задания не выполнены Обучающийся не отвечает на вопросы билета при дополнительных наводящих вопросах преподавателя.</p>	<p>Обучающийся выполнил практическое задание билета с существенными неточностями. Допускаются ошибки в содержании ответа и решении практических заданий. При ответах на дополнительные вопросы было допущено много неточностей.</p>	<p>Обучающийся выполнил практическое задание билета с небольшими неточностями. Показал хорошие умения в рамках освоенного учебного материала. Предложенные практические задания решены с небольшими неточностями. Ответил на большинство дополнительных вопросов.</p>	<p>Обучающийся правильно выполнил практическое задание билета. Показал отличные умения в рамках освоенного учебного материала. Решает предложенные практические задания без ошибок Ответил на все дополнительные вопросы.</p>

владение навыками	<p>Не может выбрать методику выполнения заданий.</p> <p>Допускает грубые ошибки при выполнении заданий, нарушающие логику решения задач.</p> <p>Делает некорректные выводы.</p> <p>Не может обосновать алгоритм выполнения заданий.</p>	<p>Испытывает затруднения по выбору методики выполнения заданий.</p> <p>Допускает ошибки при выполнении заданий, нарушения логики решения задач.</p> <p>Испытывает затруднения с формулированием корректных выводов.</p> <p>Испытывает затруднения при обосновании алгоритма выполнения заданий.</p>	<p>Без затруднений выбирает стандартную методику выполнения заданий.</p> <p>Допускает ошибки при выполнении заданий, не нарушающие логику решения задач</p> <p>Делает корректные выводы по результатам решения задачи.</p> <p>Обосновывает ход решения задач без затруднений.</p>	<p>Применяет теоретические знания для выбора методики выполнения заданий.</p> <p>Не допускает ошибок при выполнении заданий.</p> <p>Самостоятельно анализирует результаты выполнения заданий.</p> <p>Грамотно обосновывает ход решения задач.</p>
-------------------	---	--	---	---

Оценка по дисциплине зависит от уровня сформированности компетенций, закрепленных за дисциплиной, и представляет собой среднее арифметическое от выставленных оценок по отдельным результатам обучения (знания, умения, владение навыками).

Оценка «отлично»/«зачтено» выставляется, если среднее арифметическое находится в интервале от 4,5 до 5,0.

Оценка «хорошо»/«зачтено» выставляется, если среднее арифметическое находится в интервале от 3,5 до 4,4.

Оценка «удовлетворительно»/«зачтено» выставляется, если среднее арифметическое находится в интервале от 2,5 до 3,4.

Оценка «неудовлетворительно»/«не зачтено» выставляется, если среднее арифметическое находится в интервале от 0 до 2,4.

## 8. Учебно-методическое и материально-техническое обеспечение дисциплины (модуля)

### 8.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

№ п/п	Автор, название, место издания, издательство, год издания учебной и учебно-методической литературы	Количество экземпляров/электронный адрес ЭБС
<b><u>Основная литература</u></b>		
1	Башлы П. Н., Бабаш А. В., Баранова Е. К., Информационная безопасность и защита информации, Москва: Евразийский открытый институт, 2012	<a href="http://www.iprbookshop.ru/10677.html">http://www.iprbookshop.ru/10677.html</a>
2	Шаньгин В. Ф., Информационная безопасность и защита информации, Саратов: Профобразование, 2017	<a href="http://www.iprbookshop.ru/63594.html">http://www.iprbookshop.ru/63594.html</a>
3	Ильин М. Е., Ципоркова К. А., Теоретико-числовые методы в криптографии. Ч.1, Рязань: Рязанский государственный радиотехнический университет, 2020	<a href="https://www.iprbookshop.ru/121800.html">https://www.iprbookshop.ru/121800.html</a>
4	Прохорова О. В., Информационная безопасность и защита информации, Санкт-Петербург: Лань, 2023	<a href="https://e.lanbook.com/book/293009">https://e.lanbook.com/book/293009</a>
<b><u>Дополнительная литература</u></b>		

1	Шаньгин В. Ф., Защита компьютерной информации. Эффективные методы и средства, Саратов: Профобразование, 2017	<a href="http://www.iprbookshop.ru/63592.html">http://www.iprbookshop.ru/63592.html</a>
2	Скрипник Д. А., Общие вопросы технической защиты информации, Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016	<a href="http://www.iprbookshop.ru/52161.html">http://www.iprbookshop.ru/52161.html</a>

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечиваются печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

#### 8.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
SSL-сертификат. Лаборатория Касперского	<a href="https://www.kaspersky.ru/resource-center/definitions/what-is-a-ssl-certificate?srsId=AfmBOoqQp-i04crEY80D_eMrHfmBlqjtIE77IFKqdcR4PWeqtRwZSqux">https://www.kaspersky.ru/resource-center/definitions/what-is-a-ssl-certificate?srsId=AfmBOoqQp-i04crEY80D_eMrHfmBlqjtIE77IFKqdcR4PWeqtRwZSqux</a>
Блок о политике кибербезопасности. Лаборатория Касперского	<a href="https://www.kaspersky.com/about/policy-blog">https://www.kaspersky.com/about/policy-blog</a>
Безопасность операционной системы UNIX	<a href="https://uneex.ru/static/AltDocs_unix_base_admin/ch03.html">https://uneex.ru/static/AltDocs_unix_base_admin/ch03.html</a>

#### 8.3. Перечень современных профессиональных баз данных и информационных справочных систем

Наименование	Электронный адрес ресурса
Информационно-правовая система Гарант	<a href="https://www.garant.ru/products/ipo/">https://www.garant.ru/products/ipo/</a>
Информационно-правовая система Консультант	<a href="https://student2.consultant.ru/cgi/online.cgi?req=home;rnd=0.34403827862102354">https://student2.consultant.ru/cgi/online.cgi?req=home;rnd=0.34403827862102354</a>
Информационно-правовая база данных Кодекс	<a href="http://gasudata.lan.spbgasu.ru/docs/">http://gasudata.lan.spbgasu.ru/docs/</a>
Система дистанционного обучения СПбГАСУ Moodle	<a href="https://moodle.spbgasu.ru/">https://moodle.spbgasu.ru/</a>
Электронно-библиотечная система издательства "IPRsmart"	<a href="http://www.iprbookshop.ru/">http://www.iprbookshop.ru/</a>
Образовательные интернет-ресурсы СПбГАСУ	<a href="https://www.spbgasu.ru/university/obrazovatelnye-internet-resursy/">https://www.spbgasu.ru/university/obrazovatelnye-internet-resursy/</a>

#### 8.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного и свободно распространяемого программного обеспечения

Наименование	Способ распространения (лицензионное или свободно распространяемое)
Maple версия 2017	Договор №б/н от 21.06.2017 с АО "СофтЛайн Трейд". Лицензия бессрочная
Matlab версия R2019a	Договор №Д31908369487 от 01.11.2019 с ООО "Софтлайн Проекты". Лицензия до 31.12.2025
Python версия 3.7.6386.10	Свободно распространяемое
LibreOffice	Свободно распространяемое
PyCharm Community	Свободно распространяемое

## 8.5. Материально-техническое обеспечение дисциплины

### Сведения об оснащённости учебных аудиторий и помещений для самостоятельной работы

Наименование учебных аудиторий и помещений для самостоятельной работы	Оснащённость оборудованием и техническими средствами обучения
73. Помещения для самостоятельной работы	Помещение для самостоятельной работы (читальный зал библиотеки, ауд. 217): ПК-23 шт., в т.ч. 1 шт.- ПК для лиц с ОВЗ (системный блок, монитор, клавиатура, мышь) с подключением к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду СПбГАСУ.
73. Учебные аудитории для проведения лекционных занятий	Учебная аудитория для проведения занятий лекционного типа, комплект мультимедийного оборудования (персональный компьютер, мультимедийный проектор, экран, аудиосистема), доска маркерная белая эмалевая, экран, комплект учебной мебели, подключение к компьютерной сети СПбГАСУ, выход в Интернет.
73. Учебные аудитории для проведения практических занятий, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Учебная аудитория для проведения практических занятий, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации – комплект мультимедийного оборудования (персональный компьютер, мультимедийный проектор, экран, аудиосистема), доска маркерная белая эмалевая, комплект учебной мебели, подключение к компьютерной сети СПбГАСУ, выход в Интернет.
73. Компьютерный класс	Рабочие места с ПК (стол компьютерный, системный блок, монитор, клавиатура, мышь), стол рабочий, подключение к компьютерной сети СПбГАСУ, выход в Internet.

Для инвалидов и лиц с ОВЗ обеспечиваются специальные условия для получения образования в соответствии с требованиями нормативно-правовых документов.

Рабочая программа составлена на основе ФГОС ВО - бакалавриат по направлению подготовки 38.03.05 Бизнес-информатика (приказ Минобрнауки России от 29.07.2020 № 838).

Программу составил:  
доцент ИСТ, к.э.н. Яркова О.Н.

Программа обсуждена и рекомендована на заседании кафедры Информационных систем и технологий

09.09.2024, протокол № 2

Заведующий кафедрой к.э.н., доцент О.Н. Яркова

Программа одобрена на заседании учебно-методической комиссии факультета  
19.09.2024, протокол № 2.

Председатель УМК д.э.н., профессор Г.Ф. Токунова