

Федеральное государственное бюджетное образовательное учреждение высшего образования «Тамбовский государственный университет имени Г.Р. Державина»  
Институт математики, физики и информационных технологий  
Кафедра математического моделирования и информационных технологий

УТВЕРЖДАЮ:  
Директор института



Н. Л. Королева  
«04» июля 2022 г.

## **РАБОЧАЯ ПРОГРАММА**

по дисциплине Б1.В.ДВ.06.1 Криптографические протоколы

Направление подготовки/специальность: 10.03.01 - Информационная безопасность

Профиль/направленность/специализация: Безопасность компьютерных систем

Уровень высшего образования: бакалавриат

Квалификация: Бакалавр

год набора: 2022

Тамбов, 2022

**Авторы программы:**

Кандидат физико-математических наук, доцент Лопатин Дмитрий Валерьевич

Кандидат технических наук, Соловьев Денис Сергеевич

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.03.01 - Информационная безопасность (уровень бакалавриата) (приказ Министерства образования и науки РФ от «17» ноября 2020 г. № 1427).

Рабочая программа принята на заседании Кафедры математического моделирования и информационных технологий «29» июня 2022 г. Протокол № 12

Рассмотрена и одобрена на заседании Ученого совета Института математики, физики и информационных технологий, Протокол от «04» июля 2022 г. № 6.

## СОДЕРЖАНИЕ

1. Цели и задачи дисциплины.....	4
2. Место дисциплины в структуре ОП бакалавра.....	5
3. Объем и содержание дисциплины.....	5
4. Контроль знаний обучающихся и типовые оценочные средства.....	9
5. Методические указания для обучающихся по освоению дисциплины (модуля).....	15
6. Учебно-методическое и информационное обеспечение дисциплины.....	17
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	18

## 1. Цели и задачи дисциплины

### 1.1 Цель дисциплины – формирование компетенций:

ПК-1 Способен администрировать подсистемы защиты информации в операционных системах

### 1.2 Типы задач профессиональной деятельности, к которым готовятся обучающиеся в рамках освоения дисциплины:

- организационно-управленческий

1.3 Дисциплина ориентирована на подготовку обучающихся к профессиональной деятельности в сферах: 06 Связь, информационные и коммуникационные технологии (в сфере техники и технологии, охватывающей совокупность проблем, связанных с обеспечением защищенности объектов информатизации в условиях существования угроз в информационной сфере), 12 Обеспечение безопасности (в сфере защиты информации), Сфера правоохранительной деятельности

### 1.4 В результате освоения дисциплины у обучающихся должны быть сформированы:

Обобщенные трудовые функции / трудовые функции / трудовые или профессиональные действия (при наличии профстандарта)	Код и наименование компетенции ФГОС ВО, необходимой для формирования трудового или профессионального действия	Индикаторы достижения компетенций
	ПК-1 Способен администрировать подсистемы защиты информации в операционных системах	Администрирует криптографические протоколы в операционных системах

### 1.5 Согласование междисциплинарных связей дисциплин, обеспечивающих освоение компетенций:

ПК-1 Способен администрировать подсистемы защиты информации в операционных системах

№ п/п	Наименование дисциплин, определяющих междисциплинарные связи	Форма обучения				
		Очная (семестр)				
		3	4	5	6	7
1	Адаптивная Криптографические протоколы					+
2	Безопасные информационные технологии				+	+
3	На английском языке Cryptographic protocols					+
4	Ознакомительная практика				+	
5	Основы программирования в корпоративных информационных системах	+	+	+		

6	Программно-аппаратные средства защиты информации			+	+	
7	Электронная подпись					+

## 2. Место дисциплины в структуре ОП бакалавриата:

Дисциплина «Криптографические протоколы» относится к части, формируемой участниками образовательных отношений, учебного плана ОП по направлению подготовки 10.03.01 - Информационная безопасность.

Дисциплина «Криптографические протоколы» изучается в 7 семестре.

## 3. Объем и содержание дисциплины

3.1. Объем дисциплины: 2 з.е.

Очная: 2 з.е.

Вид учебной работы	Очная (всего часов)
<b>Общая трудоёмкость дисциплины</b>	<b>72</b>
Контактная работа	32
Лекции (Лекции)	16
Лабораторные (Лаб. раб.)	16
Самостоятельная работа (СР)	40
Зачет	-

## 3.2. Содержание курса:

№ темы	Название раздела/темы	Вид учебной работы, час.			Формы текущего контроля
		Лек ции	Лаб · раб.	СР	
		О	О	О	
7 семестр					
1	Протоколы обмена ключами	3	2	5	Вопросы для самоподготовки
2	Протоколы аутентификации (идентификации)	2	3	5	Вопросы для самоподготовки/Ла бораторная работа
3	Протоколы электронной подписи	2	2	6	Вопросы для самоподготовки/Ла бораторная работа
4	Протоколы контроля целостности	2	2	6	Вопросы для самоподготовки/Ла бораторная работа
5	Протоколы электронных платежей	2	2	6	Вопросы для самоподготовки
6	Протоколы голосования	2	3	6	Вопросы для самоподготовки

7	Протоколы тайных многосторонних вычислений и разделения секрета	3	2	6	Вопросы для самоподготовки/Лабораторная работа
---	---	---	---	---	--

### Тема 1. Протоколы обмена ключами

#### Лекция.

Общие положения. Алгоритм Диффи-Хеллмана-Меркла. Протокол BB84.

#### Лабораторные работы.

1. Дайте определение понятию «сеансовый ключ».
2. Опишите алгоритм обмена ключами Диффи-Хеллмана-Меркла.
3. Динамическое распределение ключей.
4. Вычисление хеш-кода ключа.
5. Что такое явная аутентификация ключа?

#### Задания для самостоятельной работы.

1. Дайте определение понятию «сеансовый ключ».
2. Опишите алгоритм обмена ключами Диффи-Хеллмана-Меркла.
3. В чем отличие квантового шифрования от квантового протокола обмена ключами.

### Тема 2. Протоколы аутентификации (идентификации)

#### Лекция.

Общие сведения, парольная идентификация / аутентификация, протокол идентификации / аутентификации с использованием хеш-функции, протокол идентификации / аутентификации на основе шифрования с открытым ключом, сервер аутентификации Kerberos, идентификация / аутентификация с помощью биометрических данных, идентификационные карты (ID-cards) и электронные ключи.

#### Лабораторные работы.

В лабораторной работе необходимо привести последовательность выполнения процедур идентификации/аутентификации с использованием следующих способов:

- на основе алгоритма RSA;
- по схеме Шнорра;
- по схеме Фейге-Фиата-Шамира.

При оформлении отчета необходимо привести таблицы генерации ключей и аутентификации. В качестве случайного числа ( $k$  или  $r$ ) принять коды, соответственно, 1-ой, 2-ой и 3-ей буквы своей фамилии согласно их положению в алфавите.

#### Задания для самостоятельной работы.

1. Дайте определение понятиям: «идентификация», «аутентификация», «авторизация».
2. Что может служить в качестве аутентификатора?
3. Перечислите основные способы организации идентификации и аутентификации.
4. Перечислите достоинства и недостатки парольной аутентификации.
5. Опишите схему протокола идентификации и аутентификации на основе алгоритма RSA.
6. В чем суть доказательства с нулевым разглашением.
7. Опишите схему протокола сервера аутентификации Kerberos.
8. Перечислите основные биометрические характеристики.

### Тема 3. Протоколы электронной подписи

#### Лекция.

Общие сведения. Протокол на базе алгоритма RSA. Алгоритм цифровой подписи ГОСТ 34.10-94. Алгоритм цифровой подписи ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012. Разновидности ЭП. Юридические основания использования ЭП.

### Лабораторные работы.

В лабораторной работе необходимо привести последовательность выполнения процедур генерации и проверки ЭЦП с использованием следующих способов:

- на базе алгоритма RSA;
- по ГОСТ 34.10-94;
- по ГОСТ 34.10-2001.

При оформлении отчета необходимо привести таблицы генерации ключей, отправки сообщения с ЭЦП и получения сообщения с ЭЦП. В качестве хеш-образа исходного сообщения  $h(T)$  принять коды, соответственно, 1-ой, 2-ой и 3-ей буквы своей фамилии согласно их положению в алфавите.

### Задания для самостоятельной работы.

1. Дайте определение понятию "электронная подпись".
2. Опишите последовательность действий участников протокола при отправке и проверке ЭП.
3. Какой порядок использования ключей (открытый; закрытый) при отправке и проверке ЭП?
4. Опишите схему протокола ЭП на основе алгоритма RSA.
5. Перечислите специальные схемы ЭП.
6. Назовите цель введения в действие Федерального закона "Об электронной подписи".

## Тема 4. Протоколы контроля целостности

### Лекция.

Общие сведения. Проверка четности. Использование контрольных цифр. Использование контрольных сумм. Использование кодов Хэмминга. Использование ЕСС. Использование ЭП. Использование MAC-кодов. Комбинированные методы (на примере жестких магнитных дисков).

### Лабораторные работы.

Задание 1:

В лабораторной работе необходимо определить контрольные данные с использованием следующих способов:

- битов четности. В качестве исходных данных принять битовое представление букв фамилии в соответствии с кодировкой Windows 1251;
  - контрольных цифр. В качестве исходных данных принять необходимое количество цифр (за исключением контрольной) из строки, состоящей из кодов букв фамилии, имени и отчества согласно их положению в алфавите:
  - по алгоритму Луна (15 цифр);
  - для штрихкода по стандарту EAN-13 (12 цифр);
  - для ИНН физического лица (10 цифр);
  - для кодов станций на железнодорожном транспорте (5 цифр);
  - контрольных сумм (CRC). В качестве исходных данных принять коды 1-ой, 2-ой и 3-ей буквы своей фамилии согласно их положению в алфавите для порождающего полинома -  $G(x) = x^4 + x^1 + x^0$ .
  - кода коррекции ошибок (ЕСС). В качестве исходных данных принять первые 11 битов первых двух букв своей фамилии в соответствии с кодировкой Windows 1251. Рассчитать вектора контрольных битов и синдромов, а также паритетные биты при отсутствии ошибки, одиночной и двойной ошибке.
- При оформлении отчета необходимо привести необходимые таблицы, исходные данные, расчеты и результаты.

Задание 2:

В лабораторной работе необходимо по алгоритму DES-CBC получить MAC-код сообщения, состоящего из первых восьми букв своей фамилии. Если количество букв в фамилии меньше 8 букв, то необходимо добавить недостающее количество букв из имени. В качестве ключа выбрать первые 7 букв сообщения; синхропосылки - 64-битовую строку из чередующихся 1 и 0 (10101010 ... 10).

При оформлении отчета необходимо привести:

- теоретическую часть, включающую "Схему шифрования блока", "Схему функции шифрования", "Схему выработки ключевых элементов" и "Схему алгоритма DES в режиме сцепления блоков шифра";

- шифруемое сообщение (8 букв фамилии) в символьном и битовом представлении в соответствии с кодировкой Windows 1251;
- синхропосылку в битовом представлении;
- результат сложения по модулю 2 шифруемого сообщения и синхропосылки;
- ключ (7 букв фамилии) в символьном и битовом представлении в соответствии с кодировкой Windows 1251;
- ключ в битовом представлении с учетом битов контроля четности;
- ключевые элементы  $k_i$ ;
- результат начальной перестановки IP;
- полублоки  $H_i$  и  $L_i$ ,  $f(k_i, L_i)$ ,  $H_i \oplus f(k_i, L_i)$ ;
- результат конечной перестановки IP-1.

#### **Задания для самостоятельной работы.**

1. Перечислите основные способы контроля целостности.
2. Что такое бит четности и как с помощью него осуществляется контроль целостности?
3. Для чего предназначена технология S.M.A.R.T.?

### **Тема 5. Протоколы электронных платежей**

#### **Лекция.**

Общие сведения, пластиковые карты, суррогатные платежные средства в Internet, расчеты пластиковыми карточками в Internet, электронные кошельки в Internet, цифровые деньги.

#### **Лабораторные работы.**

1. Перечислите основные разновидности электронных платежей.
2. В чем отличие персонафицированных платежных систем от анонимных?
3. В чем отличие дебетовых карт от кредитных?
4. Для чего используется «закрывающий множитель»?
5. Анонимные системы оплаты.

#### **Задания для самостоятельной работы.**

1. Перечислите основные разновидности электронных платежей.
2. В чем отличие персонафицированных платежных систем от анонимных?
3. В чем отличие дебетовых карт от кредитных?
4. Для чего используется «закрывающий множитель»?

### **Тема 6. Протоколы голосования**

#### **Лекция.**

Общие сведения, некоторые варианты реализации протоколов электронного голосования, российский опыт электронного голосования.

#### **Лабораторные работы.**

1. Назовите достоинства и недостатки традиционного («бумажного») голосования.
2. Что понимается под электронным голосованием?
3. Назовите основные свойства идеального протокола голосования (по Б. Шнайеру).
4. В чем отличие УСГ от КОИБ?
5. Использование электронных подписей для голосований.

#### **Задания для самостоятельной работы.**

1. Назовите достоинства и недостатки традиционного («бумажного») голосования.
2. Что понимается под электронным голосованием?
3. Назовите основные свойства идеального протокола голосования (по Б. Шнайеру).
4. В чем отличие УСГ от КОИБ?

### **Тема 7. Протоколы тайных многосторонних вычислений и разделения секрета**



### Лекция.

Тайные многосторонние вычисления. Протоколы разбиения и разделения секрета. Разбиение секрета с использованием гаммирования. Разделение секрета по схеме Шамира (интерполяционных полиномов Лагранжа). Разделение секрета по схеме Асмута-Блума. Другие разновидности схем разделения секрета.

### Лабораторные работы.

В лабораторной работе необходимо привести последовательность выполнения следующих протоколов:

- тайных многосторонних вычислений для расчета средней величины трех чисел. В качестве исходных данных принять коды 1-ой, 2-ой и 3-ей буквы своей фамилии согласно их положению в алфавите;
- разбиения секрета с использованием гаммирования для трех участников. В качестве секрета принять первые 3 буквы фамилии, для гамм - любые трехбуквенные сочетания;
- разделения секрета по схеме Шамира для (3, 5)-пороговой схемы. В качестве секрета S принять код 1-ой буквы своей фамилии согласно ее положению в алфавите;
- разделения секрета по схеме Асмута-Блума для (3, 5)-пороговой схемы. В качестве секрета S принять код 1-ой буквы своей фамилии согласно ее положению в алфавите.

При оформлении отчета необходимо привести исходные данные и таблицы, содержащие последовательность выполнения протоколов.

### Задания для самостоятельной работы.

1. Для чего необходимо применение шифрования с открытым ключом в тайных многосторонних вычислениях?
2. Что означает (m, n)-пороговая схема разделения секрета.
3. Назначение интерполяционного полинома Лагранжа.
4. Сущность китайской теоремы об остатках.

## 4. Контроль знаний обучающихся и типовые оценочные средства

### 4.1. Распределение баллов:

7 семестр

- посещаемость – 10 баллов
- текущий контроль – 50 баллов
- контрольные срезы – 2 среза по 20 баллов каждый
- премиальные баллы – 20 баллов

### Распределение баллов по заданиям:

№ темы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мах. кол-во баллов	Методика проведения занятия и оценки

1.	Протоколы обмена ключами	Вопросы для самоподготовки	10	<p>Методика оценки самоподготовки студентов.</p> <p>9 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент свободно применяет знания на практике;</li> <li>• Не допускает ошибок в воспроизведении изученного материала;</li> <li>• Студент выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы;</li> <li>• Студент усваивает весь объем программного материала.</li> </ul> <p>6 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент знает весь изученный материал;</li> <li>• Отвечает без особых затруднений на вопросы преподавателя;</li> <li>• Студент умеет применять полученные знания на практике;</li> <li>• В условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя.</li> </ul> <p>3 балла ставится тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя;</li> <li>• Предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы.</li> </ul> <p>Балл не начисляется тогда, когда:</p> <ul style="list-style-type: none"> <li>• У студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена.</li> </ul>
2.	Протоколы аутентификации (идентификации)	<b>Вопросы для самоподготовки/Лабораторная работа(контрольный срез)</b>	20	<p>Методика оценки самоподготовки студентов.</p> <p>20 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент свободно применяет знания на практике;</li> <li>• Не допускает ошибок в воспроизведении изученного материала;</li> <li>• Студент выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы;</li> <li>• Студент усваивает весь объем программного материала.</li> </ul> <p>13 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент знает весь изученный материал;</li> <li>• Отвечает без особых затруднений на вопросы преподавателя;</li> <li>• Студент умеет применять полученные знания на практике;</li> <li>• В условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя.</li> </ul> <p>5 баллов ставится тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя;</li> <li>• Предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы.</li> </ul> <p>Балл не начисляется тогда, когда:</p> <ul style="list-style-type: none"> <li>• У студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена.</li> </ul>

3.	Протоколы электронной подписи	Вопросы для самоподг отовки/Ла бораторна я работа	10	<p>Методика оценки самоподготовки студентов.</p> <p>9 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент свободно применяет знания на практике;</li> <li>• Не допускает ошибок в воспроизведении изученного материала;</li> <li>• Студент выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы;</li> <li>• Студент усваивает весь объем программного материала.</li> </ul> <p>6 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент знает весь изученный материал;</li> <li>• Отвечает без особых затруднений на вопросы преподавателя;</li> <li>• Студент умеет применять полученные знания на практике;</li> <li>• В условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя.</li> </ul> <p>3 балла ставится тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя;</li> <li>• Предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы.</li> </ul> <p>Балл не начисляется тогда, когда:</p> <ul style="list-style-type: none"> <li>• У студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена.</li> </ul>
4.	Протоколы контроля целостности	Вопросы для самоподг отовки/Ла бораторна я работа	10	<p>Методика оценки самоподготовки студентов.</p> <p>9 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент свободно применяет знания на практике;</li> <li>• Не допускает ошибок в воспроизведении изученного материала;</li> <li>• Студент выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы;</li> <li>• Студент усваивает весь объем программного материала.</li> </ul> <p>6 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент знает весь изученный материал;</li> <li>• Отвечает без особых затруднений на вопросы преподавателя;</li> <li>• Студент умеет применять полученные знания на практике;</li> <li>• В условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя.</li> </ul> <p>3 балла ставится тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя;</li> <li>• Предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы.</li> </ul> <p>Балл не начисляется тогда, когда:</p> <ul style="list-style-type: none"> <li>• У студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена.</li> </ul>

5.	Протоколы электронных платежей	Вопросы для самоподготовки(контрольный срез)	20	<p>Методика оценки самоподготовки студентов.</p> <p>20 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент свободно применяет знания на практике;</li> <li>• Не допускает ошибок в воспроизведении изученного материала;</li> <li>• Студент выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы;</li> <li>• Студент усваивает весь объем программного материала.</li> </ul> <p>13 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент знает весь изученный материал;</li> <li>• Отвечает без особых затруднений на вопросы преподавателя;</li> <li>• Студент умеет применять полученные знания на практике;</li> <li>• В условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя.</li> </ul> <p>5 баллов ставится тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя;</li> <li>• Предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы.</li> </ul> <p>Балл не начисляется тогда, когда:</p> <ul style="list-style-type: none"> <li>• У студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена.</li> </ul>
6.	Протоколы голосования	Вопросы для самоподготовки	10	<p>Методика оценки самоподготовки студентов.</p> <p>9 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент свободно применяет знания на практике;</li> <li>• Не допускает ошибок в воспроизведении изученного материала;</li> <li>• Студент выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы;</li> <li>• Студент усваивает весь объем программного материала.</li> </ul> <p>6 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент знает весь изученный материал;</li> <li>• Отвечает без особых затруднений на вопросы преподавателя;</li> <li>• Студент умеет применять полученные знания на практике;</li> <li>• В условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя.</li> </ul> <p>3 балла ставится тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя;</li> <li>• Предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы.</li> </ul> <p>Балл не начисляется тогда, когда:</p> <ul style="list-style-type: none"> <li>• У студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена.</li> </ul>

7.	Протоколы тайных многосторонних вычислений и разделения секрета	Вопросы для самоподготовки/Лабораторная работа	10	<p>Методика оценки самоподготовки студентов.</p> <p>9 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент свободно применяет знания на практике;</li> <li>• Не допускает ошибок в воспроизведении изученного материала;</li> <li>• Студент выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы;</li> <li>• Студент усваивает весь объем программного материала.</li> </ul> <p>6 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент знает весь изученный материал;</li> <li>• Отвечает без особых затруднений на вопросы преподавателя;</li> <li>• Студент умеет применять полученные знания на практике;</li> <li>• В условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя.</li> </ul> <p>3 балла ставится тогда, когда:</p> <ul style="list-style-type: none"> <li>• Студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя;</li> <li>• Предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы.</li> </ul> <p>Балл не начисляется тогда, когда:</p> <ul style="list-style-type: none"> <li>• У студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена.</li> </ul>
8.	Посещаемость		10	<p>10 баллов – студент посетил все 100% занятий 6-7 баллов – студент посетил не менее 80% занятий 4-5 баллов – студент посетил не менее 50% занятий 1-3 балла – студент посетил не менее 25% занятий Если студент посетил менее 25% занятий, баллы не начисляются.</p>
9.	Премияльные баллы		20	<p>Дополнительные премиальные баллы могут быть начислены: - за проект, выполненный по заказу работодателя и реализованный на практике – 20 баллов; - постоянная активность во время практических занятий – 10 баллов; - полностью подготовленная к публикации статья по тематике в рамках дисциплины – 10 баллов; - участие с докладом во всероссийской олимпиаде по тематике изучаемой дисциплины – 20 баллов; - участие в выставке по тематике изучаемой дисциплины – 20 баллов; - публикация статьи по тематике изучаемой дисциплины в сборнике студенческих работ / материалах всероссийской конференции</p>
10.	Итого за семестр		100	

Итоговая оценка по зачету выставляется в 100-балльной шкале и в традиционной четырехбалльной шкале. Перевод 100-балльной рейтинговой оценки по дисциплине в традиционную четырехбалльную осуществляется следующим образом:

100-балльная система	Традиционная система
50 - 100 баллов	Зачтено
0 - 49 баллов	Не зачтено

#### 4.2 Типовые оценочные средства текущего контроля

##### Вопросы для самоподготовки

##### Тема 1. Протоколы обмена ключами

1. Дайте определение понятию «сеансовый ключ».
2. Опишите алгоритм обмена ключами Диффи-Хеллмана-Меркла.
3. Опишите алгоритм обмена ключами BB84.
4. В чем отличие квантового шифрования от квантового протокола обмена ключами.
5. Уязвимости в протоколах обмена ключами.

#### Тема 5. Протоколы электронных платежей

1. Перечислите основные разновидности электронных платежей.
2. В чем отличие персонафицированных платежных систем от анонимных?
3. В чем отличие дебетовых карт от кредитных?
4. Для чего используется «закрывающий множитель»?
5. Анонимные системы оплаты.

#### Тема 6. Протоколы голосования

1. Назовите достоинства и недостатки традиционного («бумажного») голосования.
2. Что понимается под электронным голосованием?
3. Назовите основные свойства идеального протокола голосования (по Б. Шнайеру).
4. В чем отличие УСГ от КОИБ?
5. Использование электронных подписей для голосований.

### Вопросы для самоподготовки/Лабораторная работа

#### Тема 2. Протоколы аутентификации (идентификации)

1. Дайте определение понятиям: «идентификация», «аутентификация», «авторизация».
2. Что может служить в качестве аутентификатора?
3. Перечислите основные способы организации идентификации и аутентификации.
4. Перечислите достоинства и недостатки парольной аутентификации.
5. Опишите схему протокола идентификации и аутентификации на основе алгоритма RSA.
6. В чем суть доказательства с нулевым разглашением.
7. Опишите схему протокола сервера аутентификации Kerberos.
8. Перечислите основные биометрические характеристики.

#### Тема 3. Протоколы электронной подписи

1. Дайте определение понятию "электронная подпись".
2. Опишите последовательность действий участников протокола при отправке и проверке ЭП.
3. Какой порядок использования ключей (открытый; закрытый) при отправке и проверке ЭП?
4. Опишите схему протокола ЭП на основе алгоритма RSA.
5. Перечислите специальные схемы ЭП.
6. Назовите цель введения в действие Федерального закона "Об электронной подписи".

#### Тема 4. Протоколы контроля целостности

1. Перечислите основные способы контроля целостности.
2. Что такое бит четности и как с помощью него осуществляется контроль целостности?
3. Для чего предназначена технология S.M.A.R.T.?
4. Принцип работы CRC.
5. Принцип работы ESP.

#### Тема 7. Протоколы тайных многосторонних вычислений и разделения секрета

1. Для чего необходимо применение шифрования с открытым ключом в тайных многосторонних вычислениях?
2. Что означает  $(m, n)$ –пороговая схема разделения секрета.
3. Назначение интерполяционного полинома Лагранжа.
4. Сущность китайской теоремы об остатках.
5. Задача Византийских генералов.

#### 4.3 Промежуточная аттестация по дисциплине проводится в форме зачета

##### Типовые вопросы зачета (ПК-1)

1. Протоколы контроля целостности.
2. Электронные платежи.
3. Классическое ("бумажное") голосование.
4. Российский опыт электронного голосования.
5. Протокол разделения секрета.
6. Протокол подбрасывания монеты по телефону.
7. Тайные многосторонние вычисления.
8. Сложность алгоритмов.
9. Простые числа.
10. Разложение числа на простые сомножители.
11. Нахождение начального списка простых чисел.
12. Тестирование числа на простоту.
13. Определение наибольшего общего делителя.
14. Основные сведения о крипто анализе и атаки на криптосистемы.
15. Классическая стеганография.
16. Компьютерная стеганография.
17. Общие сведения о кодировании.
18. Общедоступные кодовые системы.
19. Секретные кодовые системы.

##### Типовые задания для зачета (ПК-1)

Зашифровать свою фамилию и имя с помощью шифров:

- шифра «Перекресток»;
- шифры с использованием треугольника.

#### 4.4. Шкала оценивания промежуточной аттестации

Оценка	Компетенции	Дескрипторы (уровни) – основные признаки освоения (показатели достижения результата)
«зачтено» (50 - 100 баллов)	ПК-1	
«не зачтено» (0 - 49 баллов)	ПК-1	

### 5. Методические указания для обучающихся по освоению дисциплины (модуля)

#### 5.1 Методические указания по организации самостоятельной работы обучающихся:

Приступая к изучению дисциплины, в первую очередь обучающимся необходимо ознакомиться содержанием рабочей программы дисциплины (РПД), которая определяет содержание, объем, а также порядок изучения и преподавания учебной дисциплины, ее раздела, части.

Для самостоятельной работы важное значение имеют разделы «Объем и содержание дисциплины», «Учебно-методическое и информационное обеспечение дисциплины» и «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы».

В разделе «Объем и содержание дисциплины» указываются все разделы и темы изучаемой дисциплины, а также виды занятий и планируемый объем в академических часах.

В разделе «Учебно-методическое и информационное обеспечение дисциплины» указана рекомендуемая основная и дополнительная литература.

В разделе «Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы» содержится перечень профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины.

## 5.2 Рекомендации обучающимся по работе с теоретическими материалами по дисциплине

При изучении и проработке теоретического материала необходимо:

- просмотреть еще раз презентацию лекции в системе MOODLe, повторить законспектированный на лекционном занятии материал и дополнить его с учетом рекомендованной дополнительной литературы;
- при самостоятельном изучении теоретической темы сделать конспект, используя рекомендованные в РПД источники, профессиональные базы данных и информационные справочные системы;
- ответить на вопросы для самостоятельной работы, по теме представленные в пункте 3.2 РПД.
- при подготовке к текущему контролю использовать материалы фонда оценочных средств (ФОС).

## 5.3 Рекомендации по работе с научной и учебной литературой

Работа с основной и дополнительной литературой является главной формой самостоятельной работы и необходима при подготовке к устному опросу на семинарских занятиях, к дебатам, тестированию, экзамену. Она включает проработку лекционного материала и рекомендованных источников и литературы по тематике лекций.

Конспект лекции должен содержать реферативную запись основных вопросов лекции, в том числе с опорой на размещенные в системе MOODLe презентации, основных источников и литературы по темам, выводы по каждому вопросу. Конспект может быть выполнен в рамках распечатки выдачи презентаций лекций или в отдельной тетради по предмету. Он должен быть аккуратным, хорошо читаемым, не содержать не относящуюся к теме информацию или рисунки.

Конспекты научной литературы при самостоятельной подготовке к занятиям должны содержать ответы на каждый поставленный в теме вопрос, иметь ссылку на источник информации с обязательным указанием автора, названия и года издания используемой научной литературы. Конспект может быть опорным (содержать лишь основные ключевые позиции), но при этом позволяющим дать полный ответ по вопросу, может быть подробным. Объем конспекта определяется самим студентом.

В процессе работы с основной и дополнительной литературой студент может:

- делать записи по ходу чтения в виде простого или развернутого плана (создавать перечень основных вопросов, рассмотренных в источнике);
- составлять тезисы (цитирование наиболее важных мест статьи или монографии, короткое изложение основных мыслей автора);
- готовить аннотации (краткое обобщение основных вопросов работы);
- создавать конспекты (развернутые тезисы).

## 5.4. Рекомендации по подготовке к отдельным заданиям текущего контроля

Собеседование предполагает организацию беседы преподавателя со студентами по вопросам практического занятия с целью более обстоятельного выявления их знаний по определенному разделу, теме, проблеме и т.п. Все члены группы могут участвовать в обсуждении, добавлять информацию, дискутировать, задавать вопросы и т.д.

Устный опрос может применяться в различных формах: фронтальный, индивидуальный, комбинированный. Основные качества устного ответа подлежащего оценке:

- правильность ответа по содержанию;



- полнота и глубина ответа;
- сознательность ответа;
- логика изложения материала;
- рациональность использованных приемов и способов решения поставленной учебной задачи;
- своевременность и эффективность использования наглядных пособий и технических средств при ответе;
- использование дополнительного материала;
- рациональность использования времени, отведенного на задание.

Устный опрос может сопровождаться презентацией, которая подготавливается по одному из вопросов практического занятия. При выступлении с презентацией необходимо обращать внимание на такие моменты как:

- содержание презентации: актуальность темы, полнота ее раскрытия, смысловое содержание, соответствие заявленной темы содержанию, соответствие методическим требованиям (цели, ссылки на ресурсы, соответствие содержания и литературы), практическая направленность, соответствие содержания заявленной форме, адекватность использования технических средств учебным задачам, последовательность и логичность презентуемого материала;
- оформление презентации: объем (оптимальное количество), дизайн (читаемость, наличие и соответствие графики и анимации, звуковое оформление, структурирование информации, соответствие заявленным требованиям), оригинальность оформления, эстетика, использование возможности программной среды, соответствие стандартам оформления;
- личностные качества: ораторские способности, соблюдение регламента, эмоциональность, умение ответить на вопросы, систематизированные, глубокие и полные знания по всем разделам программы;
- содержание выступления: логичность изложения материала, раскрытие темы, доступность изложения, эффективность применения средств ИКТ, способы и условия достижения результативности и эффективности для выполнения задач своей профессиональной или учебной деятельности, доказательность принимаемых решений, умение аргументировать свои заключения, выводы.

## **6. Учебно-методическое и информационное обеспечение дисциплины**

### **6.1 Основная литература:**

1. Тамб. гос. ун-т им. Г.Р. Державина, Ин-т математики, физики и информатики Техническая защита информации : учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
2. Лопатин Д.В., Калинина Ю.В. Безопасные информационные технологии : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
3. Лопатин Д. В. Программно-аппаратная защита информации : электрон. учеб. пособие. - Тамбов: [Б. и.], 2014. - 1 электрон. опт. диск (CD-ROM)
4. Лопатин Д. В. Технология информационной безопасности и методология защиты информации : электрон. учеб. пособие. - Тамбов: [Б. и.], 2014. - 1 электрон. опт. диск (CD-ROM)
5. Лопатин Д. В. Защита от вредоносных программ : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
6. Лопатин Д.В., Чиркин Е.С. Защита электронного документооборота в компьютерной системе : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)
7. Лопатин Д.В., Чиркин Е.С. Защита информационных процессов в автоматизированных системах : электрон. учеб. пособие. - Тамбов: [Б.и.], 2014. - 1 электрон. опт. диск (CD-ROM)

### **6.2 Дополнительная литература:**

1. Бехроуз, А. Криптография и безопасность сетей : учебное пособие. - 2020-11-14; Криптография и безопасность сетей. - Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. - 782 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/72337.html>

2. Аграновский, А. В., Хади, Р. А. Практическая криптография: алгоритмы и их программирование. - 2021-05-25; Практическая криптография: алгоритмы и их программирование. - Москва: СОЛОН-Пресс, 2016. - 256 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/90248.html>
3. Грибунин, В. Г., Мартынов, А. П., Николаев, Д. Б., Фомченко, В. Н. Криптография и безопасность цифровых систем : учебное пособие. - Весь срок охраны авторского права; Криптография и безопасность цифровых систем. - Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2011. - 411 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/60851.html>
4. Романьков, В. А. Алгебраическая криптография : монография. - 2023-06-30; Алгебраическая криптография. - Омск: Омский государственный университет им. Ф.М. Достоевского, 2013. - 136 с. - Текст : электронный // IPR BOOKS [сайт]. - URL: <http://www.iprbookshop.ru/24868.html>

### 6.3 Иные источники:

1. Журнал «Математические вопросы криптографии» - [http://www.mathnet.ru/php/journal.phtml?jrnid=mvk&option\\_lang=rus](http://www.mathnet.ru/php/journal.phtml?jrnid=mvk&option_lang=rus)
2. Журнал «BIS Journal - Информационная безопасность банков» - <https://journal.ib-bank.ru/pub/169>
3. Журнал «Занимательная криптография» - <https://bigmir81.livejournal.com/420975.html>
4. Блог «Криптография. Шифрование и криптоанализ» - <https://habrahabr.ru/hub/crypto/page4/>
5. Журнал «Безопасность информационных технологий» - <https://bit.mephi.ru/index.php/bit>
6. Журнал «Мир ПК» - <https://www.osp.ru/pcworld>

## 7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы

Для проведения занятий по дисциплине необходимо следующее материально-техническое обеспечение: учебные аудитории для проведения занятий лекционного и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещения для самостоятельной работы.

Учебные аудитории и помещения для самостоятельной работы укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Помещения для самостоятельной работы укомплектованы компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета.

Для проведения занятий лекционного типа используются наборы демонстрационного оборудования, обеспечивающие тематические иллюстрации (проектор, ноутбук, экран/ интерактивная доска).

Лицензионное и свободно распространяемое программное обеспечение:

Операционная система "Альт Образование"

LibreOffice

Microsoft Windows 10

Microsoft Office Профессиональный плюс 2007

Kaspersky Endpoint Security 10 для Windows "Лаборатория Касперского" 26.07.2018

Профессиональные базы данных и информационные справочные системы:

1. Электронный каталог Фундаментальной библиотеки ТГУ. – URL: <http://biblio.tsutmb.ru/elektronnyij-katalog>
2. Университетская библиотека онлайн: электронно-библиотечная система. – URL: <https://biblioclub.ru>
3. Консультант студента. Гуманитарные науки: электронно-библиотечная система. – URL: <https://www.studentlibrary.ru>
4. Научная электронная библиотека eLIBRARY.ru. – URL: <https://elibrary.ru>

5. Российская государственная библиотека. – URL: <https://www.rsl.ru>
6. Российская национальная библиотека. – URL: <http://nlr.ru>
7. Электронная библиотека РФФИ. – URL: <https://www.rfbr.ru/rffi/ru/library>

### **Электронная информационно-образовательная среда**

[https://auth.tsutmb.ru/authorize?response\\_type=code&client\\_id=moodle&state=xyz](https://auth.tsutmb.ru/authorize?response_type=code&client_id=moodle&state=xyz)

Взаимодействие преподавателя и студента в процессе обучения осуществляется посредством мультимедийных, гипертекстовых, сетевых, телекоммуникационных технологий, используемых в электронной информационно-образовательной среде университета.