

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.06.4 На английском языке Cryptographic protocols

Направление подготовки/специальность: 10.03.01 - Информационная безопасность

Профиль/направленность/специализация: Безопасность компьютерных систем

Уровень высшего образования: бакалавриат

Квалификация: Бакалавр

год набора: 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.....	16
7. Материально-техническое обеспечение дисциплины, программное обеспечение, профессиональные базы данных и информационные справочные системы.....	17

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	Криптографические протоколы					+
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 «На английском языке Cryptographic protocols» относится к части, формируемой участниками образовательных отношений, учебного плана ОП по направлению подготовки 10.03.01 - Информационная безопасность.

Дисциплина «На английском языке Cryptographic protocols» 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)
Общая трудоёмкость дисциплины	72
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	Key exchange protocols	3	2	5	Вопросы для самоподготовки
2	Authentication (identification) protocols	2	3	5	Вопросы для самоподготовки/Ла бораторная работа
3	Electronic Signature Protocols	2	2	6	Вопросы для самоподготовки/Ла бораторная работа
4	Integrity Control Protocols	2	2	6	Вопросы для самоподготовки/Ла бораторная работа
5	Electronic Payment Records	2	2	6	Вопросы для самоподготовки
6	Voting records	2	3	6	Вопросы для самоподготовки
7	Secret Multilateral Computing and Secret Separation Protocols	3	2	6	Вопросы для самоподготовки/Ла бораторная работа

Тема 1. Key exchange protocols

Лекция.

General provisions. Diffie-Hellman-Merkle algorithm. BB84 Protocol.

Лабораторные работы.

1. Define "session key."
2. Describe the Diffie-Hellman-Merkle key exchange algorithm.
3. Dynamic key distribution.
4. Calculating the key hash code.
5. What is explicit key authentication?

Задания для самостоятельной работы.

1. Define "session key."
2. Describe the Diffie-Hellman-Merkle key exchange algorithm.
3. What is the difference between quantum encryption and quantum key exchange protocol.

Тема 2. Authentication (identification) protocols**Лекция.**

General information, password identification/authentication, hash authentication/authentication protocol, public key encryption authentication/authentication protocol, Kerberos authentication server, biometric identification/authentication, ID-cards and electronic keys.

Лабораторные работы.

In the laboratory work, the sequence of identification/authentication procedures should be given using the following methods:

- based on the RSA algorithm;
- according to the Schnorr scheme;
- according to the Feige-Fiat-Shamir scheme.

When preparing a report, you must provide key generation and authentication tables. As a random number (k or r), take the codes, respectively, of the 1st, 2nd and 3rd letters of their last name according to their position in the alphabet.

Задания для самостоятельной работы.

1. Define the concepts: "identification," "authentication," "authorization."
2. What can serve as an authenticator?
3. List the main ways to organize identification and authentication.
4. List the merits and disadvantages of password authentication.
5. Describe the identification and authentication protocol scheme based on the RSA algorithm.
6. What is the essence of evidence with zero disclosure.
7. Describe the Kerberos authentication server protocol schema.
8. List the main biometric characteristics.

Тема 3. Electronic Signature Protocols**Лекция.**

General information. Protocol based on the RSA algorithm. Algorithm of digital signature GOST 34.10-94. Algorithm of digital signature GOST R 34.10-2001 and GOST R 34.10-2012. Varieties of EP. Legal grounds for using EP.

Лабораторные работы.

In the laboratory work, it is necessary to provide the sequence of execution of the EDS generation and verification procedures using the following methods:

- based on the RSA algorithm;
- as per GOST 34.10-94;
- as per GOST 34.10-2001.

When preparing the report, it is necessary to provide tables for generating keys, sending a message from the EDS and receiving a message from the EDS. As the hash image of the original message $h(T)$, accept the codes of the 1st, 2nd and 3rd letters of their last name, respectively, according to their position in the alphabet.

Задания для самостоятельной работы.

1. Define the term "electronic signature."
2. Describe the sequence of actions of the protocol participants when sending and checking the display.
3. What is the order in which the keys are used (public; closed) when sending and checking the display?
4. Describe the RSA protocol diagram.
5. List the special diagrams of the display.
6. What is the purpose of the enactment of the Federal Law "On Electronic Signature"?

Тема 4. Integrity Control Protocols

Лекция.

General information. Parity check. Use of check digits. Using checksums. Use of Hamming codes. Use of ECC. Use of EP. Using MAC codes. Combined methods (using the example of hard magnetic disks).

Лабораторные работы.

Job 1:

In laboratory work, control data must be determined using the following methods:

- parity bits. Accept the bit representation of the letters of the last name as initial data in accordance with the Windows 1251 encoding;
- check digits. As initial data, accept the required number of digits (with the exception of the control) from the line consisting of the codes of the letters of the last name, first name and patronymic according to their position in the alphabet:
 - according to the Moon algorithm (15 digits);
 - for barcode according to the EAN-13 standard (12 digits);
 - for the TIN of an individual (10 digits);
 - for railway station codes (5 digits);
- checksums (CRC). As initial data, take the codes of the 1st, 2nd and 3rd letters of your last name according to their position in the alphabet for the generating polynomial - $G(x) = x^4 + x^1 + x^0$.
- ECC code. As input, accept the first 11 bits of the first two letters of your last name according to the Windows 1251 encoding. Calculate the vectors of control bits and syndromes, as well as parity bits in the absence of error, single and double error.

When preparing the report, it is necessary to provide the necessary tables, input data, calculations and results.

Task 2:

In laboratory work, it is necessary to obtain the MAC code of a message consisting of the first eight letters of your last name using the DES-CBC algorithm. If the number of letters in the surname is less than 8 letters, then you must add the missing number of letters from the name. Select the first 7 letters of the message as the key; sync links - 64-bit string of interleaved 1 and 0 (10101010... 10).

When preparing the report, it is necessary to provide:

- theoretical part including "Block Encryption Scheme," "Encryption Function Scheme," "Key Element Generation Scheme" and "DES Algorithm Scheme in Cipher Block Coupling Mode";
- an encrypted message (8 letters of the last name) in character and bit representation in accordance with the Windows 1251 encoding;
- synchronous message in bit representation;
- result of modulo 2 addition of the encrypted message and sync link;
- key (7 letters of last name) in character and bit representation in accordance with Windows 1251 encoding;
- key in bit representation taking into account parity bits;
- key elements k_i ;
- result of initial IP permutation;

- half blocks H_i and L_i , $f(k_i, L_i)$, $H_i \oplus f(k_i, L_i)$;
- is the result of a finite permutation of the IP-1.

Задания для самостоятельной работы.

1. List the main ways to monitor integrity.
2. What is the parity bit and how is it used to monitor integrity?
3. What is the purpose of S.M.A.R.T. technology?

Тема 5. Electronic Payment Records

Лекция.

General information, plastic cards, surrogate payment means in the Internet, settlements with plastic cards in the Internet, electronic wallets in the Internet, digital money.

Лабораторные работы.

1. List the main types of electronic payments.
2. What is the difference between personalized payment systems and anonymous ones?
3. What's the difference between debit cards and credit cards?
4. What is the closing factor used for?
5. Anonymous payment systems.

Задания для самостоятельной работы.

1. List the main types of electronic payments.
2. What is the difference between personalized payment systems and anonymous ones?
3. What's the difference between debit cards and credit cards?
4. What is the closing factor used for?

Тема 6. Voting records

Лекция.

General information, some options for implementing electronic voting protocols, Russian experience in electronic voting.

Лабораторные работы.

1. Name the advantages and disadvantages of traditional ("paper") voting.
2. What is meant by electronic voting?
3. Name the basic properties of an ideal voting protocol (according to B. Schneier).
4. What is the difference between USG and KOIB?
5. Use of electronic signatures for votes.

Задания для самостоятельной работы.

1. Name the advantages and disadvantages of traditional ("paper") voting.
2. What is meant by electronic voting?
3. Name the basic properties of an ideal voting protocol (according to B. Schneier).
4. What is the difference between USG and KOIB?

Тема 7. Secret Multilateral Computing and Secret Separation Protocols

Лекция.

Clandestine multilateral computing. Secret partitioning and partitioning protocols. Breaking a secret using gamming. Separation of the secret according to the Shamir scheme (Lagrange interpolation polynomials). Asmuth-Bloom secrecy separation. Other varieties of secret separation schemes.

Лабораторные работы.

The following protocols shall be followed in laboratory work:

- secret multilateral calculations for calculating the average of three numbers. As initial data, accept the codes of the 1st, 2nd and 3rd letters of your last name according to their position in the alphabet;

- secret partitioning with the use of gamming for three participants. As a secret, take the first 3 letters of the surname, for scales - any three-letter combinations;
- separation of the secret according to the Shamir scheme for the (3, 5) threshold scheme. As a secret, S adopt the code of the 1st letter of his surname according to its position in the alphabet;
- Asmuth-Bloom secret separation for (3, 5) threshold scheme. As a secret, S accept the code of the 1st letter of his surname according to its position in the alphabet.

When preparing the report, it is necessary to provide initial data and tables containing the sequence of protocol execution.

Задания для самостоятельной работы.

1. Why do I need to use public key encryption in clandestine multi-party computing?
2. Which is the (m, n) threshold secret separation scheme.
3. Purpose of the Lagrange interpolation polynomial.
4. Essence of the Chinese residue theorem.

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:

№ те мы	Название темы / вид учебной работы	Формы текущего контроля / срезы	Мах. кол-во баллов	Методика проведения занятия и оценки
1.	Key exchange protocols	Вопросы для самоподготовки	10	<p>Методика оценки самоподготовки студентов.</p> <p>9 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> • Студент свободно применяет знания на практике; • Не допускает ошибок в воспроизведении изученного материала; • Студент выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы; • Студент усваивает весь объем программного материала. <p>6 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> • Студент знает весь изученный материал; • Отвечает без особых затруднений на вопросы преподавателя; • Студент умеет применять полученные знания на практике; • В условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя. <p>3 балла ставится тогда, когда:</p> <ul style="list-style-type: none"> • Студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя; • Предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы. <p>Балл не начисляется тогда, когда:</p> <ul style="list-style-type: none"> • У студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена.

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

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

6.	Voting records	Вопросы для самоподготовки	10	<p>Методика оценки самоподготовки студентов.</p> <p>9 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> • Студент свободно применяет знания на практике; • Не допускает ошибок в воспроизведении изученного материала; • Студент выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы; • Студент усваивает весь объем программного материала. <p>6 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> • Студент знает весь изученный материал; • Отвечает без особых затруднений на вопросы преподавателя; • Студент умеет применять полученные знания на практике; • В условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя. <p>3 балла ставится тогда, когда:</p> <ul style="list-style-type: none"> • Студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя; • Предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы. <p>Балл не начисляется тогда, когда:</p> <ul style="list-style-type: none"> • У студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена.
7.	Secret Multilateral Computing and Secret Separation Protocols	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"> • Студент свободно применяет знания на практике; • Не допускает ошибок в воспроизведении изученного материала; • Студент выделяет главные положения в изученном материале и не затрудняется в ответах на видоизмененные вопросы; • Студент усваивает весь объем программного материала. <p>6 баллов ставятся тогда, когда:</p> <ul style="list-style-type: none"> • Студент знает весь изученный материал; • Отвечает без особых затруднений на вопросы преподавателя; • Студент умеет применять полученные знания на практике; • В условных ответах не допускает серьезных ошибок, легко устраняет определенные неточности с помощью дополнительных вопросов преподавателя. <p>3 балла ставится тогда, когда:</p> <ul style="list-style-type: none"> • Студент обнаруживает освоение основного материала, но испытывает затруднения при его самостоятельном воспроизведении и требует дополнительных дополняющих вопросов преподавателя; • Предпочитает отвечать на вопросы воспроизводящего характера и испытывает затруднения при ответах на воспроизводящие вопросы. <p>Балл не начисляется тогда, когда:</p> <ul style="list-style-type: none"> • У студента имеются отдельные представления об изучаемом материале, но все, же большая часть не усвоена.
8.	Посещаемость		10	<p>10 points - the student attended all 100% of classes 6-7 points - the student attended at least 80% of classes 4-5 points - the student attended at least 50% of classes 1-3 points - the student attended at least 25% of classes If the student attended less than 25% of classes, points are not awarded.</p>

9.	Премияльные баллы	20	Additional bonus points can be awarded: - for a project commissioned by the employer and implemented in practice - 20 points; - constant activity during practical exercises - 10 points; - fully prepared for publication article on subjects within the discipline - 10 points; - participation with a report in the All-Russian Olympiad on the subject of the studied discipline - 20 points; - participation in the exhibition on the subject of the studied discipline - 20 points; - publication of an article on the subject of the studied discipline in the collection of student works/materials of the All-Russian Conference
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. Key exchange protocols

1. Дайте определение понятию «сеансовый ключ».
2. Опишите алгоритм обмена ключами Диффи-Хеллмана-Меркла.

Тема 5. Electronic Payment Records

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

Тема 6. Voting records

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. Authentication (identification) protocols

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. Electronic Signature Protocols

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. Integrity Control Protocols

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. Secret Multilateral Computing and Secret Separation Protocols

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. Integrity control protocols.
2. Electronic payments.
3. Classic ("paper") voting.
4. Russian experience of electronic voting.
5. Secret separation protocol.
6. Coin toss protocol over the phone.
7. Clandestine multilateral computing.
8. Complexity of algorithms.
9. Primes.
10. Decomposition of a number into prime multipliers.
11. Find the initial list of primes.
12. Testing the number for simplicity.
13. Determination of the largest common divisor.
14. Basic information about crypto analysis and attacks on cryptosystems.
15. Classical steganography.
16. Computer steganography.
17. General Coding Information.
18. Public code systems.
19. Secret code systems.

Типовые задания для зачета (ПК-1)

Encrypt your last name and first name using ciphers:

- cipher "Crossroads";
- are ciphers using a triangle.

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
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

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