Аннотация

Дисциплина «Криптографические протоколы» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 10.03.01 «Информационная безопасность» направленности/специализации «Безопасность компьютерных систем». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ОПК-9 «Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности»

ОПК-1.1 «Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах»

ОПК-1.2 «Способен администрировать средства защиты информации в компьютерных системах и сетях»

Содержание дисциплины охватывает круг вопросов, связанных с основами криптологии, базовыми криптографическими примитивами, синтезом и анализом стойкости криптографических протоколов.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа обучающегося.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме экзамена (7 семестр).

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов.

Язык обучения по дисциплине «русский »

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Целями преподавания дисциплины «Криптографические протоколы» являются формирование у студентов теоретических знаний и практических навыков по основам криптологии, базовым криптографическим примитивам, по синтезу и анализу стойкости криптографических протоколов.

1.2. Дисциплина входит в состав обязательной части образовательной программы высшего образования (далее – ОП ВО).

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП ВО.

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями или их частями. Компетенции и индикаторы их достижения приведены в таблице 1.

Таблица 1 – Перечень компетенций и индикаторов их достижения

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Общепрофессиональные компетенции	ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.З.3 знает основные понятия и задачи криптографии, математические модели криптографических систем ОПК-9.З.4 знает основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и криптографические протоколы ОПК-9.З.5 знает национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения ОПК-9.У.2 умеет применять математические модели для оценки стойкости СКЗИ ОПК-9.У.3 умеет использовать СКЗИ в автоматизированных системах
Общепрофессиональные компетенции по направленности	ОПК-1.1 Способен разрабатывать и реализовывать политики управления доступом в компьютерных системах	ОПК-1.1.З.3 знает принципы функционирования сетевых протоколов, включающих криптографические алгоритмы ОПК-1.1.У.2 умеет использовать криптографические протоколы, применяемые в компьютерных сетях
Общепрофессиональные компетенции по направленности	ОПК-1.2 Способен администрировать средства защиты информации в компьютерных системах и сетях	ОПК-1.2.З.2 знает принципы функционирования программных средств криптографической защиты информации

2. Место дисциплины в структуре ОП

Дисциплина может базироваться на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

– «Математические основы криптологии»,

– «Алгоритмические проблемы криптографии».

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и могут использоваться при написании выпускной квалификационной работы.

3. Объем и трудоемкость дисциплины

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 2.

Таблица 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№7
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	3/ 108	3/ 108
Из них часов практической подготовки		
Аудиторные занятия, всего час.	68	68
в том числе:		
лекции (Л), (час)	34	34
практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	34	34
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)	36	36
Самостоятельная работа, всего (час)	4	4
***Вид промежуточной аттестации*:** зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.)	Экз.,	Экз.,

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий.

Разделы, темы дисциплины и их трудоемкость приведены в таблице 3.

Таблица 3 – Разделы, темы дисциплины, их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП/КР (час)	СР (час)
Семестр 7					
Раздел 1. Криптографические алгоритмы Тема 1.1 – Основные понятия криптографииТема 1.2 – Симметричные криптосистемы Тема 1.3 – Контроль целостности Тема 1.4 – Основные алгоритмы с открытымключом	16		16		2

Раздел 2. Криптографические протоколыТема 1.1 – Управление ключами Тема 1.2 – Протоколы цифровых денег иэлектронного голосования Тема 1.3 – Протоколы идентификации иличностная криптография Тема 1.4 – Постквантовая криптография	16		18		2
Итого в семестре:	34		34		4
Итого	34	0	34	0	4

Практическая подготовка заключается в непосредственном выполнении обучающимися определенных трудовых функций, связанных с будущей профессиональной деятельностью.

4.2. Содержание разделов и тем лекционных занятий.

Содержание разделов и тем лекционных занятий приведено в таблице 4.

Таблица 4 – Содержание разделов и тем лекционного цикла

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	Раздел 1. Криптографические алгоритмы Тема 1.1 – Основные понятия криптографии: История, терминология, классификация шифров, понятие ключа и основные задачи (конфиденциальность, целостность, аутентификация). Тема 1.2 – Симметричные криптосистемы: Принципы шифрования с одним ключом, блочные и потоковые шифры, стандарты (DES, AES, ГОСТ). Тема 1.3 – Контроль целостности: Хэш-функции, коды аутентификации сообщений (MAC) и их применение для защиты от модификации данных. Тема 1.4 – Основные алгоритмы с открытым ключом: Асимметричное шифрование, алгоритмы RSA, Эль-Гамаля и эллиптические кривые.
2	Раздел 2. Криптографические протоколы Тема 1.1 – Управление ключами: Методы распределения, генерации и хранения ключей, инфраструктура открытых ключей (PKI), схемы Диффи-Хеллмана. Тема 1.2 – Протоколы цифровых денег и электронного голосования: Использование криптографии в блокчейне, криптографические валюты и анонимные платежные системы, принципы тайного голосования. Тема 1.3 – Протоколы идентификации и личностная криптография: Электронная цифровая подпись (ЭЦП), биометрическая идентификация и доказательства с нулевым разглашением. Тема 1.4 – Постквантовая криптография: Алгоритмы, устойчивые к атакам с использованием квантовых компьютеров (решетчатая, хеш- и код-базовая криптография).

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Учебным планом не предусмотрено					
Всего					

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 6.

Таблица 6 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 7				
1	Исследование классических методов шифрования: шифр Цезаря и шифр Виженера	4		1
2	Реализация и исследование режимов работы блочного шифра AES (ГОСТ Р 34.12-2015)	4		1
3	Вычисление хэш-функций и проверка целостности файлов с помощью утилит семейства SHA	4		1
4	Генерация ключей и шифрование данных по алгоритму RSA	4		1
5	Реализация протокола Диффи-Хеллмана для безопасного обмена ключами	4		2
6	Моделирование транзакций в упрощенной блокчейн-сети	4		2
7	Создание и верификация электронной цифровой подписи (ЭЦП)	4		2
8	Тестирование постквантового алгоритма шифрования Kyber	6		2
Всего		34		

4.5. Выполнение курсового проекта/ курсовой работы

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 7, час
1	2	3
Изучение теоретического материала дисциплины (ТО)		
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	2	2
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	2	2
Всего:	4	4

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. разделов 6-11.

6. Перечень печатных и электронных учебных изданий

Перечень печатных и электронных учебных изданий приведен в таблице 8.

Таблица 8– Перечень печатных и электронных учебных изданий

Шифр/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004.4 К 84	Крук, Е. А. Методы программирования и прикладные алгоритмы [Текст]: учебное пособие в3 ч. Ч. 1 / Е. А. Крук, А. А. Овчинников; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб.:Изд-во ГУАП, 2014. - 178 с.	40
Х М 48	Информационная безопасность и защита информации [Текст]: учебноепособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков; ред. С. АКлейменов. - 5-е изд., стер. - М.: Академия, 2011. - 331 с.	25
http://e.lanbook.com/view/book/1540/	Глухов М. М., Круглов И. А., ПичкурА. Б., Черемушкин А. В. Введение в теоретико-числовые методы криптографии. Лань, 2011.	

7. Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

URL адрес	Наименование
Lms.guap.ru	Система дистанционного обучения ГУАП (СДО ГУАП)
rsv.ru	Платформа “Россия – страна возможностей”
leader-id.ru	Платформа “Leader-ID”

8. Перечень информационных технологий

8.1. Перечень программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине.

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

8.2. Перечень информационно-справочных систем,используемых при осуществлении образовательного процесса по дисциплине

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория	
2	Мультимедийная лекционная аудитория	

10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средствдля проведения промежуточной аттестации обучающихся по дисциплине приведен в таблице 13.

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Экзамен	Список вопросов к экзамену; Экзаменационные билеты*; Задачи;

	Тесты.

Примечание: *экзаменационные билеты формируются на основе вопросов и задач таблицы 15.

10.2. В качестве критериев оценки уровня сформированности (освоения) компетенций обучающимися применяется 5-балльная шкала оценки сформированности компетенций, которая приведена в таблице 14. В течение семестра может использоваться 100-балльная шкала модульно-рейтинговой системы Университета, правила использования которой, установлены соответствующим локальным нормативным актом ГУАП.

Таблица 14 –Критерии оценки уровня сформированности компетенций

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«отлично» «зачтено»	Обучающийся: – глубоко и всесторонне усвоил программный материал; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно связывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий. – правильно выполнил от 90% до 100% тестовых заданий**.
«хорошо» «зачтено»	Обучающийся: – твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; – не допускает существенных неточностей; – увязывает усвоенные знания с практической деятельностью направления; – аргументирует научные положения; – делает выводы и обобщения; – владеет системой специализированных понятий. – правильно выполнил от 70% до 89% тестовых заданий**.
«удовлетворительно» «зачтено»	– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; – допускает несущественные ошибки и неточности; – испытывает затруднения в практическом применении знаний направления; – слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий. – правильно выполнил от 51% до 69% тестовых заданий**.
«неудовлетворительно» «не зачтено»	– обучающийся не усвоил значительной части программного материала; – допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; – испытывает трудности в практическом применении знаний; – не может аргументировать научные положения; – не формулирует выводов и обобщений. – правильно выполнил менее 51% тестовых заданий**.

10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена	Код

		индикатора
1	Задача обеспечения секретности. Шифры подстановок. Примеры. Шифры перестановок. Примеры.	ОПК-9.З.3
2	Стойкость шифров. Модели атакующего Симметричные блоковые шифры. Свойства, принципыпостроения.	ОПК-9.З.4
3	Итеративные блоковые шифры. Сети Файстеля.Примеры.	ОПК-9.З.5
4	Шифр DES. Шифр ГОСТ 28147-89. Шифр FEALШифр IDEA.Шифр AES.	ОПК-9.У.2
5	Режимы блокового шифрования. Регистры сдвига с линейной обратной связью. Алгоритм Берлекэмпа-Мэсси. Потоковые шифры. Свойства, принципы построения.	ОПК-9.У.3
6	Хэш-функции, свойства, принципы построения. MDC, MAC Задача идентификации. Парольная идентификация Асимметричные шифры. Свойства, принципы построения.	ОПК-1.1.З.3
7	Система RSA. Система Эль-Гамаля Система Меркли-Хеллмана Система Мак-Элиса Задача обеспечения аутентификации. Цифровая подпись.	ОПК-1.1.У.2
8	Подпись RSA. Подпись DSA Подпись Эль-Гамаля. Подпись ГОСТ Р 34.10-94 Распределение ключей. Протокол Диффи-Хеллмана. Цифровой конверт Распределение ключей. Сертификаты.	ОПК-1.2.З.2

Вопросы (задачи) для зачета / дифф. зачета представлены в таблице 16.

Таблица 16 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета	Код индикатора
	Учебным планом не предусмотрено	

Перечень тем для выполнения курсового проекта/ курсовой работы представлены в таблице 17.

Таблица 17 – Перечень тем для выполнения курсового проекта / курсовой работы

№ п/п	Примерный перечень тем для выполнения курсового проекта/ курсовой работы
	Учебным планом не предусмотрено

Вопросы для проведения промежуточной аттестации в виде тестирования представлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
1	**Вопрос 1:** Какое свойство безопасности гарантирует, что конфиденциальная информация не станет доступной неавторизованным	ОПК-9.З.3

	лицам? А) Целостность Б) Конфиденциальность В) Аутентификация Г) Доступность **Правильный ответ:** Б **Вопрос 2:** Как называется криптоаналитическая атака, при которой у злоумышленника есть доступ только к зашифрованному тексту, без знания исходного текста или ключа? А) Атака на основе известного открытого текста (Known-plaintext) Б) Атака на основе подобранного открытого текста (Chosen-plaintext) В) Атака на основе только шифртекста (Ciphertext-only) Г) Атака «человек посередине» (Man-in-the-middle) **Правильный ответ:** В	
2	**Вопрос 3:** Какой размер блока данных (в битах) использует современный стандарт симметричного шифрования AES? А) 64 бита Б) 128 бит В) 256 бит Г) 512 бит **Правильный ответ:** Б **Вопрос 4:** Какой режим работы блочного шифра превращает его в потоковый, шифруя последовательность инициализирующих векторов и складывая результат по модулю 2 (XOR) с открытым текстом? А) ECB (Electronic Codebook) Б) CBC (Cipher Block Chaining) В) OFB (Output Feedback) или CTR (Counter) Г) Режим простой замены **Правильный ответ:** В	ОПК-9.З.4
3	**Вопрос 5:** Какое свойство криптографической хэш-функции означает, что вычислительно невозможно найти два разных исходных сообщения, которые дают одинаковый хэш-код? А) Устойчивость к поиску первого прообраза Б) Устойчивость к коллизиям (второго рода) В) Лавинный эффект Г) Необратимость **Правильный ответ:** Б **Вопрос 6:** В чем главное отличие кода аутентификации сообщения (MAC) от обычной хэш-функции (например, SHA-256)? А) MAC работает быстрее Б) Для вычисления MAC используется секретный ключ В) MAC имеет меньшую длину выхода Г) MAC применяется только для шифрования файлов **Правильный ответ:** Б	ОПК-9.З.5
4	**Вопрос 7:** На какой труднорешаемой математической задаче основана криптографическая стойкость алгоритма RSA? А) Задача дискретного логарифмирования Б) Задача факторизации (разложения на множители) больших целых чисел В) Задача поиска кратчайшего вектора в решетке Г) Задача изогении эллиптических кривых **Правильный ответ:** Б **Вопрос 8:** Каким ключом отправитель должен **зашифровать** сообщение в асимметричной системе, чтобы его мог прочесть только получатель? А) Своим закрытым ключом Б) Своим открытым ключом	ОПК-9.У.2

	В) Открытым ключом получателя Г) Закрытым ключом получателя **Правильный ответ:** В	
5	**Вопрос 9:** Какую основную задачу решает классический протокол Диффи-Хеллмана (Diffie-Hellman)? А) Шифрование больших объемов данных Б) Формирование общей цифровой подписи В) Безопасная генерация общего секретного ключа по незащищенному каналу Г) Проверка подлинности веб-сайтов **Правильный ответ:** В **Вопрос 10:** Какую функцию в инфраструктуре открытых ключей (PKI) выполняет Удостоверяющий центр (CA)? А) Хранит закрытые ключи всех пользователей Б) Выпускает и подписывает цифровые сертификаты, связывающие личность с открытым ключом В) Осуществляет автоматическое шифрование трафика Г) Генерирует одноразовые пароли для авторизации **Правильный ответ:** Б	ОПК-9.У.3
6	**Вопрос 11:** Какая криптографическая технология позволяет скрыть связь между монетой и её владельцем при создании цифровых денег, обеспечивая анонимность? А) Симметричное шифрование AES Б) Слепая подпись (Blind signature) В) Обычный хэш-код SHA-3 Г) Протокол Диффи-Хеллмана **Правильный ответ:** Б **Вопрос 12:** Какое свойство протоколов электронного голосования гарантирует, что никто (даже администратор системы) не сможет узнать, за кого проголосовал конкретный избиратель, но голос будет учтен? А) Неотказуемость Б) Доступность В) Тайность голосования при проверяемости (End-to-end verifiability) Г) Синхронность **Правильный ответ:** В	ОПК-1.1.З.3
7	**Вопрос 13:** С помощью какого ключа создается (вычисляется) электронная цифровая подпись (ЭЦП) под документом? А) С помощью открытого ключа отправителя Б) С помощью закрытого ключа отправителя В) С помощью открытого ключа получателя Г) С помощью сессионного ключа **Правильный ответ:** Б **Вопрос 14:** Как называются криптографические протоколы, которые позволяют одной стороне (доказывающей) убедить другую сторону (проверяющую) в истинности утверждения (например, в знании пароля), не раскрывая самой информации? А) Протоколы с нулевым разглашением (Zero-Knowledge Proofs) Б) Протоколы разделения секрета В) Протоколы аутентификации Kerberos Г) Протоколы сквозного шифрования **Правильный ответ:** А	ОПК-1.1.У.2
8	**Вопрос 15:** Какое устройство в будущем сможет за полиномиальное время взломать классические асимметричные алгоритмы (RSA, ECC) с помощью алгоритма Шора? А) Нейроморфный процессор Б) Суперкомпьютер на базе GPU	ОПК-1.2.З.2

	В) Квантовый компьютер Г) Оптический компьютер **Правильный ответ:** В **Вопрос 16:** Какой класс математических задач чаще всего используется для построения современных постквантовых алгоритмов шифрования (например, Kyber/ML-KEM)? А) Задачи на эллиптических кривых Б) Задачи факторизации В) Задачи на математических решетках (Lattice-based cryptography) Г) Задачи дискретного логарифмирования в конечных полях **Правильный ответ:** В	

Перечень тем контрольных работ по дисциплине обучающихся заочной формы обучения, представлены в таблице 19.

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
	Не предусмотрено

10.4. Методические материалы, определяющие процедуры оценивания индикаторов, характеризующих этапы формирования компетенций, содержатся в локальных нормативных актах ГУАП, регламентирующих порядок и процедуру проведения текущего контроля успеваемости и промежуточной аттестации обучающихся ГУАП.

11. Методические указания для обучающихся по освоению дисциплины

11.1. Методические указания для обучающихся по освоению лекционного материала.

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемые результаты при освоении обучающимися лекционного материала:

– получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;

– получение опыта творческой работы совместно с преподавателем;

– развитие профессионально-деловых качеств, любви к предмету и самостоятельного творческого мышления.

– появление необходимого интереса, необходимого для самостоятельной работы;

– получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;

– научиться методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);

– получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала:

Каждый лекционный комплекс (или отдельная лекция) оформляется по следующему шаблону:

1. Титульная часть и метаданные

- **Название темы:** Четкая формулировка (например, *«Тема 1.4 – Основные алгоритмы с открытым ключом»*).
- **Цель лекции:** Какую главную проблему решает данная тема.
- **Задачи лекции:** Чему студент научится (знать, уметь, владеть).
- **План лекции:** Краткий перечень рассматриваемых вопросов (3–4 пункта).

2. Вводная часть (Актуализация)

- **Связь с прошлым материалом:** Короткое напоминание, на какие ранее изученные темы опирается лекция.
- **Проблематика:** Описание уязвимости или практической проблемы, которую невозможно решить старыми методами (например, проблема передачи секретного ключа по открытому каналу перед изучением асимметричного шифрования).

3. Основная теоретическая часть

Это ядро лекции, разбитое строго по пунктам плана:

- **Базовые понятия и определения:** Введение новых терминов, математического аппарата или стандартов.
- **Анатомия алгоритма/протокола:** Пошаговое описание работы схемы (например: Генерация ключей Шифрование Расшифрование).
- **Графические схемы и диаграммы:** Визуализация потоков данных, взаимодействия сторон (особенно критично для раздела *«Криптографические протоколы»*).
- **Криптостойкость и ограничения:** Анализ уязвимостей, стойкость к атакам (включая квантовые для темы 2.4), требования к длине ключей.

4. Практико-ориентированный блок

- **Примеры применения:** Где это используется в реальном мире (SSL/TLS, блокчейн, ГОСТ, банковские смарт-карты).
- **Численный пример:** Разбор работы алгоритма «на пальцах» с минимальными цифровыми значениями (например, расчет RSA для простых чисел \(p=3, q=11\)).

5. Заключительная часть (Контроль и рефлексия)

- **Выводы:** Краткое резюме лекции в 2–3 предложениях.
- **Вопросы для самопроверки:** 3–5 концептуальных вопросов для закрепления материала.
- **Связь с практикой:** Анонс лабораторной работы, которая будет выполняться по этой теме.

6. Информационное обеспечение

- **Основная литература:** Учебники, профильные стандарты (ГОСТы, RFC).
- **Дополнительные ресурсы:** Ссылки на симуляторы, криптографические библиотеки или актуальные исследования.

11.2. Методические указания для обучающихся по выполнению лабораторных работ

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом, и относится к средствам, обеспечивающим решение следующих основных задач обучающегося:

– приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;

– закрепление, развитие и детализация теоретических знаний, полученных на лекциях;

– получение новой информации по изучаемой дисциплине;

– приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание и требования к проведению лабораторных работ

Регламент выполнения работ направлен на развитие практических навыков программирования и анализа криптографических систем.

- **Самостоятельность выполнения:** Каждая работа выполняется студентом индивидуально. Использование чужого программного кода (плагиат) ведет к аннулированию результатов.
- **Среда реализации:** Программный код пишется на согласованном с преподавателем языке (рекомендуется **Python**, **C++** или **Go**) с минимальным использованием сторонних высокоуровневых библиотек (если цель работы — реализация алгоритма «с нуля»).
- **Входной контроль (Допуск):** Перед началом работы студент обязан пройти устный опрос по теоретическому материалу соответствующей лекции.
- **Защита работы:** Для успешной сдачи студент демонстрирует работающее приложение на различных (включая критические) наборах входных данных и отвечает на контрольные вопросы преподавателя.
- **Сроки сдачи:** Работа должна быть защищена в течение **14 календарных дней** с момента ее выдачи по графику. Несвоевременная сдача снижает итоговый балл.

Структура и форма отчета о лабораторной работе

Отчет является основным документом, подтверждающим выполнение задания, и должен содержать строго определенные разделы.

- **Титульный лист:** Официальное наименование вуза, кафедры, дисциплины, номер и тема работы, ФИО студента и преподавателя, город и год.
- **Цель и задачи работы:** Формулировка учебных и практических целей, а также перечень конкретных задач для их достижения.
- **Краткие теоретические сведения:** Описание математического аппарата, стандартов шифрования или структуры протокола в объеме 1–2 страниц (не копировать лекцию целиком).
- **Постановка задачи (Индивидуальное задание):** Описание конкретного варианта задания, выданного преподавателем, включая исходные данные.
- **Алгоритм и листинг программы:**
- Текстовое описание или блок-схема логики работы программы.
- Исходный код ключевых функций с подробными комментариями.
- **Результаты работы и тестирования:** Скриншоты интерфейса или консоли, демонстрирующие корректность работы (например: исходный текст => расшифрованный текст).
- **Выводы:** Анализ полученных результатов, оценка криптостойкости или производительности реализованного метода, подтверждение достижения цели.

Требования к оформлению отчета о лабораторной работе

Оформление отчета должно строго соответствовать стандартам **ГОСТ 7.32** (для РФ) или внутренним академическим нормативам.

- **Параметры страницы и шрифта:**
- Шрифт: **Times New Roman**, кегль **14 pt** (для кода в листингах допускается Courier New, 10–12 pt).
- Межстрочный интервал: **1.5**.
- Выравнивание: По ширине страницы, с абзацным отступом **1.25 см**.
- Поля: Левое — 30 мм, правое — 15 мм, верхнее и нижнее — 20 мм.
- **Нумерация страниц:** Сквозная, арабскими цифрами внизу страницы по центру. На титульном листе номер не ставится, но включается в общую нумерацию.
- **Формулы и математические выражения:**
- Все формулы должны быть набраны в стандартном редакторе формул (или в системе LaTeX с использованием символов $ для встроенного текста и $$ для выделенных блоков).
- Большие формулы нумеруются арабскими цифрами в круглых скобках у правого края страницы.
- **Иллюстрации и таблицы:**

- Скриншоты и диаграммы подписываются снизу по центру: *«Рисунок 1 – Результат шифрования файла»*.
- Таблицы подписываются сверху слева: *«Таблица 1 – Сравнительный анализ скорости работы алгоритмов»*.
- На все рисунки и таблицы в тексте обязаны быть ссылки (например: *«...как показано на рисунке 1»*).
- **Формат файла:** Готовый отчет сохраняется и отправляется на проверку исключительно в формате **PDF** (исходные файлы кода прикрепляются отдельно или загружаются в репозиторий Git).

11.3. Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

В процессе выполнения самостоятельной работы у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет ему развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихсяявляются:

– учебно-методический материал по дисциплине;

– методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

11.4. Методические указания для обучающихся по прохождению текущего контроля успеваемости.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины.

Текущий контроль по данной дисциплине базируется на балльно-рейтинговой системе и состоит из трех основных блоков: тестирования, защиты лабораторных работ и активности на лекционных занятиях.

Оценка успеваемости формируется накопительным методом. Примерная структура распределения рейтинговых баллов (максимум — 100 баллов за семестр):

```
[Текущий контроль: 100 баллов]
  ├── Лабораторные работы (8 работ по 7 баллов) ──> 56 баллов
  ├── Тестирование (2 теста по 12 баллов) ──────────> 24 баллов
  ├── Экспресс-опросы / Аудиторная работа ──────────> 10 баллов
  └── Индивидуальное творческое задание / Реферат ─> 10 баллов
```

Блок 1. Лабораторный практикум (56 баллов)

Подготовка: До начала занятия студент обязан изучить методические указания к работе, повторить лекционный материал и подготовить проект (программный код или схему).

Входной контроль: Проводится в форме блиц-опроса (до 5 минут). Студент должен объяснить суть изучаемого алгоритма (например, структуру раунда AES или математическую основу RSA).

Сдача кода: Студент демонстрирует преподавателю работу программы. Обязательна проверка на различных тестовых векторах и граничных условиях.

Защита отчета: Студент предоставляет отчет, оформленный по ГОСТу, и отвечает на контрольные вопросы по модификации кода или анализу уязвимостей реализованного протокола.

Блок 2. Тестирование (24 балла)

В семестре проводятся два обязательных рубежных теста (по одному на каждый раздел дисциплины) в электронной образовательной среде:

Тест №1: Криптографические алгоритмы (проводится на 8–9 неделе).

Тест №2: Криптографические протоколы (проводится на 16–17 неделе).

Условия: На выполнение теста из 16–20 вопросов отводится ровно 30 минут. Допускается только одна попытка. Использование конспектов и сети Интернет блокируется системой прокторинга.

Блок 3. Аудиторная и самостоятельная работа (20 баллов)

Блиц-опросы на лекциях: Короткие письменные или устные опросы в начале лекции по материалу предыдущего занятия (оценивается понимание терминологии).

Индивидуальное задание: Подготовка аналитического доклада или мини-исследования по современным криптографическим стандартам или инцидентам безопасности (например, анализ реальной атаки на протокол TLS).

Критерии оценки лабораторной работы (макс. 7 баллов):

7 баллов: Работа сдана в срок. Программа работает без ошибок, код оптимален и прокомментирован. Студент уверенно отвечает на все теоретические и практические вопросы, свободно владеет математическим аппаратом алгоритма. Отчет оформлен идеально.

5–6 баллов: Работа сдана в срок, но есть незначительные замечания к структуре кода или оформлению отчета. Студент ответил на большинство вопросов с небольшими подсказками преподавателя.

3–4 балла: Работа сдана с опозданием (по графику дедлайнов) ИЛИ в коде присутствуют логические ошибки, интерфейс нестабилен. Студент испытывает серьезные трудности при объяснении работы собственного алгоритма.

0 баллов: Программа не работает, обнаружен плагиат (копирование чужого кода) или студент не явился на защиту.

Критерии оценки рубежного тестирования:

90% – 100% правильных ответов — отлично (максимальный балл за тест).

75% – 89% правильных ответов — хорошо.

60% – 74% правильных ответов — удовлетворительно.

Менее 60% — неудовлетворительно (тест считается непройденным, требуется пересдача в установленные дни).

11.5. Методические указания для обучающихся по прохождению промежуточной аттестации.

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

– экзамен – форма оценки знаний, полученных обучающимся в процессе изучения всей дисциплины или ее части, навыков самостоятельной работы, способности применять их для решения практических задач. Экзамен, как правило, проводится в период экзаменационной сессии и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Допуск к экзамену

Для получения официального допуска к сдаче экзамена студент обязан выполнить минимальные требования учебного плана в течение семестра:

- **Выполнить и защитить все 8 лабораторных работ** с предоставлением оформленных по ГОСТу отчетов в формате PDF.
- **Пройти оба рубежных теста** (по Разделам 1 и 2) с оценкой не ниже «удовлетворительно» (минимум 60% правильных ответов).

- **Набрать минимальный пороговый балл** по балльно-рейтинговой системе (если в вузе применяется БРС, обычно это не менее 40–50 баллов из 100 возможных за семестр).
  Студенты, не выполнившие лабораторный практикум, к экзамену не допускаются до момента ликвидации академической задолженности.

Форма и регламент проведения экзамена

Экзамен проводится в устно-письменной форме по экзаменационным билетам.

- **Состав билета:** Каждый билет содержит **3 вопроса**:

1. *Вопрос 1 (Теоретический):* Из Раздела 1 «Криптографические алгоритмы».
2. *Вопрос 2 (Теоретический):* Из Раздела 2 «Криптографические протоколы».
3. *Вопрос 3 (Практический):* Задача на расчет криптографических параметров или разбор уязвимости протокола.

- **Регламент времени:**
  - На подготовку ответов (написание конспекта ответа на экзаменационном листе) отводится **45 минут**.
  - На устный ответ и собеседование с экзаменатором — до **15 минут**.
- **Запрещенные материалы:** Во время экзамена категорически запрещено использовать учебники, конспекты лекций, мобильные телефоны, шпаргалки и любые программируемые устройства. Обнаружение любых вспомогательных средств ведет к немедленному удалению с экзамена с выставлением оценки «неудовлетворительно».

Критерии оценивания ответов на экзамене

Итоговая оценка за экзамен (или финальный балл с учетом семестровой работы) выставляется на основе следующих критериев:

- **Оценка «Отлично» (High Pass / A):**
  - Студент демонстрирует глубокие системные знания по обоим теоретическим вопросам.
  - Свободно оперирует терминами, безошибочно воспроизводит математический аппарат шифров (например, формулы RSA, Diffie-Hellman) и схемы взаимодействия сторон в протоколах.
  - Практическое задание выполнено полностью и без ошибок, даны исчерпывающие пояснения.
  - Студент уверенно и аргументированно отвечает на любые дополнительные вопросы.
- **Оценка «Хорошо» (Pass / B-C):**
  - Студент твердо знает материал, грамотно излагает суть криптографических алгоритмов и протоколов.
  - В ответах отсутствуют грубые ошибки, однако допущены мелкие неточности или пробелы в деталях (например, не полностью описаны все раунды блочного шифра или режимы его работы).
  - Практическое задание решено верно, но студент испытывает небольшие затруднения при обосновании промежуточных шагов.
- **Оценка «Удовлетворительно» (Low Pass / D-E):**
  - Студент обладает лишь базовыми знаниями по вопросам билета, понимает общие принципы (например, понимает разницу между симметричным и асимметричным шифрованием), но не помнит конкретных формул или стандартов.
  - Изложение материала поверхностное, фрагментарное.
  - Практическое задание выполнено частично или с грубыми ошибками.
  - Ответ на дополнительные вопросы возможен только при наводящих вопросах экзаменатора.
- **Оценка «Неудовлетворительно» (Fail / F):**
  - Студент имеет серьезные пробелы в базовых понятиях криптографии, не может объяснить принципы работы ключевых алгоритмов.
  - Практическая задача не решена, понимание алгоритма решения отсутствует.
  - Ответы на дополнительные и наводящие вопросы не получены.

Рекомендации по подготовке к экзамену

- **Систематизируйте материал по парам «Теория – Практика»:** При подготовке к теоретическому вопросу всегда вспоминайте, какую лабораторную работу вы выполняли по этой

теме. Практический опыт реализации (например, Kyber или блокчейна) поможет восстановить в памяти теорию.

- **Учите математические основы:** Обратите особое внимание на базовые операции модульной арифметики (нахождение обратного элемента по модулю, возведение в степень по модулю), свойства простых чисел и эллиптических кривых. Без них сдать Раздел 1 на высокую оценку невозможно.
- **Визуализируйте протоколы:** При подготовке вопросов из Раздела 2 (электронные деньги, голосование, идентификация) обязательно зарисовывайте на черновике схемы обмена сообщениями между условными участниками (Alice, Bob, Trent). Это упрощает устный ответ.
- **Используйте официальные стандарты:** При повторении алгоритмов (AES, ГОСТ Р 34.12-2015, SHA-256) опирайтесь на спецификации и стандарты, так как экзаменатор может спросить точные технические характеристики (размеры ключей, блоков, количество раундов).

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой