

**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**
**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»**
(СПбГУТ)

Кафедра Безопасности информационных систем
(полное наименование кафедры)

УТВЕРЖДЕН

на заседании кафедры

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Криптографическая защита информации
(наименование дисциплины)

09.03.02 Информационные системы и технологии
(код и наименование направления подготовки / специальности)

Технологии проектирования защищенных систем обработки данных
(направленность / профиль образовательной программы)

1. Общие положения

Фонд оценочных средств (ФОС) по дисциплине используется в целях нормирования процедуры оценивания качества подготовки и осуществляет установление соответствия учебных достижений запланированным результатам обучения и требованиям образовательной программы дисциплины.

Предметом оценивания являются знания, умения, навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций у обучающихся.

Процедуры оценивания применяются в процессе обучения на каждом этапе формирования компетенций посредством определения для отдельных составных частей дисциплины методов контроля - оценочных средств.

Основным механизмом оценки качества подготовки и формой контроля учебной работы студентов являются текущий контроль успеваемости и промежуточная аттестация. Общие требования к процедурам проведения текущего контроля и промежуточной аттестации определяет внутренний локальный акт университета: Положение о текущем контроле успеваемости и промежуточной аттестации обучающихся. При проведении текущего контроля успеваемости и промежуточной аттестации студентов используется ФОС.

1.1. Цель и задачи текущего контроля студентов по дисциплине.

Цель текущего контроля - систематическая проверка степени освоения программы дисциплины «Криптографическая защита информации», уровня достижения планируемых результатов обучения - знаний, умений, навыков в ходе ее изучения при проведении занятий, предусмотренных учебным планом.

Задачи текущего контроля:

1. обнаружение и устранение пробелов в освоении учебной дисциплины;
2. своевременное выполнение корректирующих действий по содержанию и организации процесса обучения;
3. определение индивидуального учебного рейтинга студентов;
4. подготовка к промежуточной аттестации.

В течение семестра при изучении дисциплины реализуется традиционная система поэтапного оценивания уровня освоения. За каждый вид учебных действий студенты получают оценку .

1.2. Цель и задачи промежуточной аттестации студентов по дисциплине.

Цель промежуточной аттестации - проверка степени усвоения студентами учебного материала, уровня достижения планируемых результатов обучения и сформированности компетенций на момент завершения изучения дисциплины.

Промежуточная аттестация проходит в форме зачета.

Задачи промежуточной аттестации:

1. определение уровня освоения учебной дисциплины;
2. определение уровня достижения планируемых результатов обучения и сформированности компетенций;
3. соотнесение планируемых результатов обучения с планируемыми результатами освоения образовательной программы в рамках изученной дисциплины.

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

2.1.Перечень компетенций.

ПК-31 Способность обеспечивать информационную безопасность хранилищ и баз данных, баз знаний

УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач

2.2.Этапы формирования компетенций.

Таблица 1

Код компетенции	Этап формирования компетенции	Вид учебной работы	Тип контроля	Форма контроля
ПК-31, УК-1	теоретический (информационный)	лекции, самостоятельная работа	текущий	тест
	практико-ориентированный	практические (лабораторные) занятия, самостоятельная работа	текущий	тест, домашнее задание
	оценочный	аттестация	промежуточный	зачет

Применяемые образовательные технологии определяются видом контактной работы.

2.3.Соответствие разделов дисциплины формируемым компетенциям.

Этапами формирования компетенций является взаимосвязанная логическая последовательность освоения разделов (тем) учебной дисциплины.

Таблица 2

№ п/п	Раздел (тема) дисциплины	Содержание раздела (темы) дисциплины	Коды компетенций
1	Раздел 1. Основные понятия и задачи криптографии	Основные понятия криптографии и криптоанализа: криптографическое преобразование информации, отправитель и получатель информации, канал связи, открытое сообщение, криптографический ключ, процессы шифрования и расшифрования, криптограмма, криптографическая система, противник и его атаки. Методы криптографической защиты информации и роль криптографии в обеспечении безопасности информации. Основные задачи криптографии: обеспечение установленного режима доступа к информации, обеспечение целостности информации, аутентификация автора сообщения. История криптографии. Классические шифры. Шифры замены и перестановки. Классические шифры перестановки: «Сцитала», табличные перестановки, поворотные решетки. Криптоанализ простых шифров перестановки.	ПК-31, УК-1

2	Раздел 2. Шифры. Симметричные криптосистемы	Блочные и потоковые шифры. Классификация шифров замены. Шифры одноалфавитной (простой) замены. Криптосистема Цезаря. Частотный анализ шифров простой замены. Перестановки. Моноалфавитные и многоалфавитные подстановки. Системы шифрования Виженера. Псевдослучайные генераторы. Гаммирование. Стандарты шифрования AES и ГОСТ. Моноалфавитные и многоалфавитные подстановки. Системы шифрования Виженера. Псевдослучайные генераторы. Алгоритмы гаммирования. Стандарты шифрования.	ПК-31, УК-1
3	Раздел 3. Модели асимметричных криптосистем.	Двух-ключевые системы шифрации. Системы шифрования с открытым ключом. Однонаправленные функции. Алгоритм RSA. Криптографические хэш функции. Криптосистемы на эллиптических ключах. Изучение асимметричных криптосистем, процедур аутентификации и ЭЦП. Криптосистемы без передачи ключей.	ПК-31, УК-1
4	Раздел 4. Электронная подпись	Коды аутентичности сообщений. Электронная подпись. ГОСТ Р 34.10-2012. DSS. Инфраструктура открытого ключа.	ПК-31, УК-1
5	Раздел 5. Криптографические протоколы	Основные понятия. Понятие криптографического протокола. Свойства, характеризующие безопасность протоколов. Виды криптографических протоколов. Основные атаки на безопасность протоколов. Протоколы сертификации ключей, протоколы распределения ключей.	ПК-31, УК-1
6	Раздел 6. Основы стеганографии	Стеганография в XXI веке. Цели. Практическое применение. Актуальность.	ПК-31, УК-1

3. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

3.1. Описание показателей оценивания компетенций на различных этапах их формирования.

Таблица 3

Код компетенции	Показатели оценивания (индикаторы достижения компетенций)	Оценочные средства
------------------------	--	---------------------------

ПК-31	<p>ПК-31.1 Знать: угрозы и мероприятия по обеспечению информационной безопасности хранилищ и баз данных, баз знаний;</p> <p>ПК-31.2 Уметь: выявлять угрозы и разрабатывать мероприятия по обеспечению информационной безопасности хранилищ и баз данных, баз знаний;</p> <p>ПК-31.3 Иметь навыки: идентификации угроз и реализации мероприятий по обеспечению информационной безопасности хранилищ и баз данных, баз знаний;</p>	<p>ТЕОРЕТИЧЕСКИЙ ЭТАП: тест</p> <p>ПРАКТИКО-ОРИЕНТИРОВАННЫЙ ЭТАП: тест, домашнее задание</p> <p>ОЦЕНОЧНЫЙ ЭТАП: вопросы к зачету</p>
УК-1	<p>УК-1.1 Знать: методики поиска, сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа.;</p> <p>УК-1.2 Уметь: применять методики поиска, сбора и обработки информации; осуществлять критический анализ и синтез информации, полученной из разных источников; применять системный подход для решения поставленных задач.;</p> <p>УК-1.3 Владеть: методами поиска, сбора и обработки, критического анализа и синтеза информации; методикой системного подхода для решения поставленных задач.;</p>	<p>ТЕОРЕТИЧЕСКИЙ ЭТАП: тест</p> <p>ПРАКТИКО-ОРИЕНТИРОВАННЫЙ ЭТАП: тест, домашнее задание</p> <p>ОЦЕНОЧНЫЙ ЭТАП: вопросы к зачету</p>

3.2. Стандартные критерии оценивания.

Критерии разработаны с учетом требований ФГОС ВО к конечным результатам обучения и создают основу для выявления уровня сформированности компетенций: минимального, базового или высокого.

Критерии оценки ответа за зачет:

Для зачета в устном виде :

- логика при изложении содержания ответа на вопрос, выявленные знания соответствуют объему и глубине их раскрытия в источнике;
- использование научной терминологии в контексте ответа;
- объяснение причинно-следственных и функциональных связей;
- умение оценивать действия субъектов социальной жизни, формулировать собственные суждения и аргументы по определенным проблемам;
- эмоциональное богатство речи, образное и яркое выражение мыслей.

Критерии оценки тестового контроля знаний:

студентом даны правильные ответы на

- 91-100% заданий - отлично,
- 81-90% заданий - хорошо,
- 71-80% заданий - удовлетворительно,
- 70% заданий и менее - неудовлетворительно.

Общие критерии оценки работы студента на практических занятиях:

- Отлично - активное участие в обсуждении проблем каждого семинара, самостоятельность ответов, свободное владение материалом, полные и аргументированные ответы на вопросы семинара, участие в дискуссиях, твердое знание лекционного материала, обязательной и рекомендованной дополнительной литературы, регулярная посещаемость занятий.

- Хорошо - недостаточно полное раскрытие некоторых вопросов темы, незначительные ошибки в формулировке категорий и понятий, меньшая активность на семинарах, неполное знание дополнительной литературы, хорошая посещаемость.
- Удовлетворительно - ответы отражают в целом понимание темы, знание содержания основных категорий и понятий, знакомство с лекционным материалом и рекомендованной основной литературой, недостаточная активность на занятиях, оставляющая желать лучшего посещаемость.
- Неудовлетворительно - пассивность на семинарах, частая неготовность при ответах на вопросы, плохая посещаемость.

Порядок применения критериев оценки конкретизирован ниже, в разделе 4, содержащем оценочные средства для текущего контроля успеваемости и для проведения промежуточной аттестации студентов по данной дисциплине.

3.3. Описание шкал оценивания.

В процессе оценивания результатов обучения и компетенций на различных этапах их формирования при освоении дисциплины для всех перечисленных выше оценочных средств используется шкала оценивания, приведенная в таблице 4.

Дихотомическая шкала оценивания используется при проведении текущего контроля успеваемости студентов: при проведении собеседования, при приеме эссе, реферата, а также может быть использована в целях проведения такой формы промежуточной аттестации, как зачет (шкала приводится для всех оценочных средств из таблицы 3).

Таблица 5

Показатели оценивания	Описание в соответствии с критериями оценивания	Оценка знаний, умений, навыков и опыта	Оценка по дихотомической шкале
Высокий уровень освоения	Демонстрирует полное понимание проблемы. Требования по всем критериям выполнены	«очень высокая», «высокая»	«зачтено»
Базовый уровень освоения	Демонстрирует значительное понимание проблемы. Требования по всем критериям выполнены	«достаточно высокая», «выше средней», «базовая»	«зачтено»
Минимальный уровень освоения	Демонстрирует частичное понимание проблемы. Требования по большинству критериев выполнены	«средняя», «ниже средней», «низкая», «минимальная»	«зачтено»
Недостаточный уровень освоения	Демонстрирует небольшое понимание проблемы. Требования по многим критериям не выполнены	«очень низкая», «примитивная»	«незачтено»

4. Типовые контрольные задания, иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

4.1.Оценочные средства промежуточной аттестации

Оценочные средства промежуточной аттестации по дисциплине представлены в Приложении 1.

4.2.Формирование тестового задания промежуточной аттестации Аттестация №1

В экзаменационном билете присутствует 3 вопроса теоретической и практической направленности. Теоретические вопросы позволяют оценить уровень знаний и частично - умений, практические - уровень умений и владения компетенцией.

Примерный перечень заданий, выносимых на промежуточную аттестацию, разрешенных учебных и наглядных пособий, средств материально-технического обеспечения и типовые практические задания (задачи):

По вопросу 1, компетенции ПК-31,УК-1

- 1 Криптографическое преобразование информации, отправитель и получатель информации
- 10 Табличные перестановки, поворотные решетки
- 20 Стандарт шифрования AES

По вопросу 2, компетенции ПК-31,УК-1

- 1 Обобщенная модель стегосистемы
- 7 Алгоритм RSA
- 13 Криптографические хэш функции

По вопросу 3, компетенции ПК-31,УК-1

- Расшифруйте следующие сообщения, зашифрованные шифром Цезаря, и определите ключ n , $0 < n < 33$, если известно, что исходные сообщения составлены из алфавита АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ: а) ЮВПЛШУХ б) СФЫЮБШЯФУ
- 2 Сложите по модулю 28: о двоичные числа 10101100 и 11001010; 0111 0110 о десятичные числа 155 и 100; $1001\ 1011 + 01100100 = 1111\ 1111 - 255$ о шестнадцатеричные числа 0B5 и 37. ЕС Примечание: десятичные числа необходимо сначала перевести в двоичный вид.
 - 10 Пусть хеш-функция $y = h(x_1x_2...x_n)$ определяется как результат выполнения побитовой операции "сумма по модулю 2" для всех байтов сообщения, представленного в двоичном виде. Длина хеш-кода равна 8 битам. Для каждого из шести сообщений, записанных в левом столбце, найдите соответствующий результат вычисления хеш-функции из правого столбца. Сообщение и значение хеш-функции представлены в шестнадцатеричном формате. Определить Хеш-функцию сообщения DA 14 90

Представленный по каждому вопросу перечень заданий является рабочей моделью для генерирования экзаменационных билетов.

4.3.Развернутые критерии выставления оценки

Таблица 6

Тип вопроса	Показатели оценки			
	5	4	3	2
Теоретические вопросы	тема разносторонне проанализирована, ответ полный, ошибок нет, предложены обоснованные аргументы и приведены примеры эффективности аналогичных решений	тема разносторонне раскрыта, ответ полный, допущено не более 1 ошибки, предложены обоснованные аргументы и приведены примеры эффективности аналогичных решений	тема освещена поверхностно, ответ полный, допущено более 2 ошибок, обоснованных аргументов не предложено	ответы на вопрос билета практически не даны
Практические вопросы	задание выполнено без ошибок, студент может дать все необходимые пояснения, сделать выводы	задание выполнено без ошибок, но студент не может пояснить ход выполнения и сделать необходимые выводы	задание выполнено с одной ошибкой, при ответе на вопрос ошибка замечена и исправлена самостоятельно	задание невыполнено или выполнено с двумя и более ошибками, пояснения к ходу выполнения недостаточны
Дополнительные вопросы	ответы даны на все вопросы, показан творческий подход	ответы даны на все вопросы, творческий подход отсутствует	ответы на дополнительные вопросы ошибочны (2 и более ошибок)	ответы на дополнительные вопросы практически отсутствуют
Уровень освоения	высокий	базовый	минимальный	недостаточный

Для получения оценки «зачтено» студент должен показать уровень освоения всех компетенций, предусмотренных программой данной дисциплины, не ниже минимального.

4.4. Комплект экзаменационных билетов

Комплект экзаменационных билетов ежегодно обновляется и формируется перед зачетом.

Развернутые критерии выставления оценки за зачет содержатся в таблице 5.

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и/или опыта деятельности, характеризующих этапы формирования компетенций

5.1. Методические материалы для текущего контроля успеваемости

Текущий контроль предусматривает систематическое оценивание процесса

обучения, с учетом необходимости обеспечения достижения обучающимися планируемых результатов обучения по дисциплине (уровня сформированности знаний, умений, навыков, компетенций), а также степени готовности обучающихся к профессиональной деятельности. Система текущего контроля успеваемости и промежуточной аттестации студентов предусматривает решение следующих задач:

- оценка качества освоения студентами основной профессиональной образовательной программы;
- аттестация студентов на соответствие их персональных достижений поэтапным требованиям соответствующей основной профессиональной образовательной программы;
- поддержание постоянной обратной связи и принятие оптимальных решений в управлении качеством обучения студентов на уровне преподавателя, кафедры, факультета и университета.

В начале учебного изучения дисциплины преподаватель проводит входной контроль знаний студентов, приобретённых на предшествующем этапе обучения.

Задания, реализуемые только при проведении текущего контроля

Тест - система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.

5.2. Методические материалы для промежуточной аттестации

Форма промежуточной аттестации по дисциплине - зачет

Форма проведения зачета: устная

При подготовке к ответу на зачете студент, как правило, ведет записи в листе устного ответа, который затем (по окончании зачета) сдается экзаменатору.

Экзаменатору предоставляется право задавать обучающимся дополнительные вопросы в рамках программы дисциплины текущего семестра, а также, помимо теоретических вопросов, давать задачи, которые изучались на практических занятиях.

Основой для определения оценки служит уровень усвоения студентами материала, предусмотренного рабочей программой дисциплины. Знания, умения, навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций у обучающихся, определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» или «зачтено», «не зачтено».

Выбор формы оценивания определяется целями и задачами обучения. В числе применяемых форм оценивания выделяют интегральную и дифференцируемую оценку, а также самоанализ и самоконтроль студента. Источники информации, которые используются при применении разных форм оценивания:

- работы обучающихся: домашние задания, презентации, отчеты, дневники, эссе и т.п.;
- результаты индивидуальной и совместной деятельности студентов в процессе обучения;
- результаты выполнения контрольных работ, тестов;
- другие источники информации.

Для того чтобы оценка выполняла те функции, которые на нее возложены как на

характеристику этапов формирования компетенций у обучающихся, необходимо соблюдение следующих базовых принципов оценивания:

- непрерывность процесса оценивания;
- оценивание должно быть критериальным, основанным на целях обучения;
- критерии выставления оценки и алгоритм ее выставления должны быть заранее известны;
- включение обучающихся в контрольно-оценочную деятельность.

Конечный результат обучения (с точки зрения соответствия его заявленным целям) в высокой степени определяется набором критериальных показателей, которые используются в процессе оценки.

Студенту, использующему в ходе зачета неразрешенные источники и средства для получения информации, выставляется неудовлетворительная оценка. В случае неявки студента на зачет преподавателем делается в экзаменационной ведомости отметка «не явился».