Приложение А

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА» (СПбГУТ)

Кафедра Защищенных систем связи
(полное наименование кафедры)

УТВЕРЖДЕН

на заседании кафедры № 6 от 13.06.2018

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Криптографические протоколы
(наименование дисциплины)

10.05.02 Информационная безопасность телекоммуникационных систем
(код и наименование направления подготовки / специальности)

Безопасность телекоммуникационных систем информационного взаимодействия
(направленность / профиль образовательной программы)

Санкт-Петербург

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 «Криптографические протоколы», 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.

ОПК-2 способностью применять соответствующий математический аппарат для решения профессиональных задач

ПК-2 способностью формулировать задачи, планировать и проводить исследования, в том числе эксперименты и математическое моделирование, объектов, явлений и процессов телекоммуникационных систем, включая обработку и оценку достоверности их результатов

2.2.Этапы формирования компетенций.

Таблица 1

Код компетенции	Этап формирования компетенции	Вид учебной работы	Тип контроля	Форма контроля
ОПК-2, ПК-2	теоретический (информационный)	лекции, самостоятельная работа	текущий	собеседование
	практико-ориентированный	практические (лабораторные) занятия, самостоятельная работа	текущий	домашнее задание
	оценочный	аттестация	промежу-точный	зачет

Применяемые образовательные технологии определяются видом контактной работы.

2.3.Соответствие разделов дисциплины формируемым компетенциям.

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

Таблица 2

№ п/п	Раздел (тема) дисциплины	Содержание раздела (темы) дисциплины	Коды компетенций
1	Раздел 1. Принципы построения систем шифрования	Введение в криптографию. Типы криптосистем. Модель системы шифрования. Способы шифрования. Влияние ошибок в криптограмме на дешифрование.	ОПК-2
2	Раздел 2. Безусловностойкие криптосистемы	Необходимые и достаточные условия построения безусловно стойких криптосистем. Понятие расстояния единственности. Вывод формулы для расстояния единственности для произвольного шифра и ее анализ.	ОПК-2
3	Раздел 3. Блочные шифры	Принципы построения блочных шифров. Шифры на основе схемы Фейстеля. Подстановочно перестановочные шифры. Методы криптоанализа блочных шифров: тотальный перебор ключей, анализ статистики криптограммы, линейный и дифференциальный. Модификации блоковых шифров. Стандарты шифрования AES, ГОСТ 3 34.12-15.	ОПК-2

4	Раздел 4. Потоковые шифры	Принципы построения потоковых шифров. Линейный рекуррентный регистр и его свойства. Нелинейные узлы усложнения, используемые для построения потоковых шифров. Нерегулярное тактирование в потоковых шифрах. Основные методы криптоанализа потоковых шифров. Анализ шифра А5 стандарта GSM.	ПК-2
5	Раздел 5. Аутентификация сообщений	Модель системы аутентификации, классификация, характеристики эффективности. Безусловно стойкие системы аутентификации. Вычислительно-стойкие системы аутентификации. Способы построения ключевых хэш-функций. Системы аутентификации, на основе блочного шифра.	ПК-2
6	Раздел 6. Управление ключами в симметричных криптосистемах	Модель управления ключами. Этапы жизненного цикла ключа. Распределение ключей на основе ЦРК и доверенных каналов. Распределение ключей в интерактивном режиме с использованием ЦРК.	ПК-2

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 компе-тенции	Показатели, критерии оценивания (планируемые результаты обучения)	Оценочные средства
ОПК-2	ЗНАЕТ: принципы построения криптосистем с открытым ключом; УМЕЕТ: рассчитывать основные характеристики и параметры криптографических алгоритмов защиты информации; ВЛАДЕЕТ: приемами проектирования типовых алгоритмов криптозащиты и криптоанализа сообщений;	ТЕОРЕТИЧЕСКИЙ ЭТАП: собеседование ПРАКТИКО-ОРИЕНТИРОВАННЫЙ ЭТАП:защита, домашнее задание ОЦЕНОЧНЫЙ ЭТАП: вопросы к зачету
ПК-2	ЗНАЕТ: Принципы построения ключевых хэш-функций; УМЕЕТ: оценивать (в первом приближении) стойкость основных криптосистем и их элементов; ВЛАДЕЕТ: методами компьютерного моделирования алгоритмов шифрования и расшифрования сообщений;	ТЕОРЕТИЧЕСКИЙ ЭТАП: собеседование ПРАКТИКО-ОРИЕНТИРОВАННЫЙ ЭТАП:защита, домашнее задание ОЦЕНОЧНЫЙ ЭТАП: вопросы к зачету

Критерии, указанные в таблице 3, разработаны с учетом требований ФГОС ВО к конечным результатам обучения и создают основу для выявления уровня сформированности компетенций: минимального, базового или высокого.

3.2.Стандартные критерии оценивания.

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 лабораторной работы:

- Выполнение лабораторной работы (подготовленность к выполнению, осознание цели работы, методов собирания схемы, проведение измерений и фиксирования их результатов, прилежание, самостоятельность выполнения, наличие и правильность оформления необходимых материалов для проведения работы – схема соединений, таблицы записей и т.п.);
- Оформление отчета по лабораторной работе (аккуратность оформления результатов измерений, правильность вычислений, правильность выполнения графиков, векторных диаграмм и др.) ;
- Правильность и самостоятельность выбора формул для расчетов при оформлении результатов работы;
- Правильность построения графиков, умение объяснить их характер;
- Правильность построения векторных диаграмм, умение их строить и понимание того, что они значат;
- Ответы на контрольные вопросы к лабораторной работе.

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, твёрдое 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 посещаемостью
- 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, отсутствие качеств, указанных выше для получения более высоких оценок.

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 .

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 4

Показатели оценивания	**Описание в соответствии с критериями оценивания, приведенными в таблице 3**	**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 текущего контроля успеваемости

Оценочные средства текущего контроля успеваемости по дисциплине представлены в Приложении 1.

4.2.Формирование тестового задания промежуточной аттестации

Аттестация №1

В экзаменационном билете присутствует 2 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 ОПК-2

1 Понятие теоретически недешифруемых систем.
2 Проблемы оценки стойкости современных криптосистем.
3 Модель шифрования - расшифрования дискретных сообщений.
4 Необходимое условие построения ТНДШ систем.
5 ТНДШ системы. Свойства. Особенности применения.
6 Способы определения расстояния единственности. Примеры.
7 Понятие расстояния единственности.
8 Сведения из теории сложности. Понятие о простых и сложных алгоритмах.
9 Свойства потоковых шифров и примеры использования. Построение потокового шифра на основе блокового.
10 Потоковые шифры Методы формирования шифрующей последовательности. ЛРР (использование в потоковых шифрах).
11 Потоковые шифры (методы построения, свойства, примеры).
12 Способы реализации преобразований в блоковых шифрах. Структура Файстеля. Примеры использования.
13 Модульная арифметика (нахождение обратного элемента по модулю, функция Эйлера, малая теорема Ферма, тесты на простоту).
14 Основные типы преобразований при построении блоковых шифров.
15 Многократное шифрование. Свойства. Особенности использования.
16 Принципы построения блоковых шифров.
17 Понятие хеш функции. Применение в цифровой подписи. Требования к хеш-функции.
18 Вычислительно стойкие криптосистемы
19 Криптосистема Эль-Гамаля. Сравнение симметричных и асимметричных криптосистем. (Свойства асимметричных криптосистем).
20 Модульная арифметика (понятие о модульной арифметике, сложение, умножение, возведение в степень, логарифмирование, факторизация, НОД).
21 Параметры наиболее известных блоковых шифров.
22 Модификация с зацеплением блоков.
23 Управление ключами. Понятие мастер ключа и сессионных ключей. Способы хранения ключей.
24 Методы распределение ключей. Непосредственное распределение ключей.
25 Атака на потоковый шифр при неизменной гамме.
26 Методы распределения ключей на основе физических особенностей канала связи.
27 Дополнительные криптографические протоколы. Обеспечение безопасности взаимодействия пользователей.
28 Цифровая подпись. Алгоритмы реализации цифровой подписи. Стандарты цифровой подписи.
29 Принципы построения асимметричных криптосистем.
30 Потенциальные атаки на RSA. Нахождение секретного ключа, слабые просты числа.

По вопросу 2, компетенции ОПК-2

1 Определить среднее количество коллизий при использовании хеширования с длиной хеша 10 бит для сообщений длиной 22 бита.
2 Найти значения следующих выражений: 3^10 mod11, 3^24 mod35, 4*2^(-1)mod5.
3 Определить итоговый ключ в алгоритме Диффи-Хелмана, если заданы открытые параметры a=3 и модуль преобразований p=31, секретные числа пользователей A и B составляют 5 и 7 соответственно.
4 Определить количество единиц на периоде выходной последовательности ЛРР заданного следующим полиномом: h(x)=x^4+x+1.
5 Определить количество необходимое количество шагов для выполнения алгоритма разложения на множители методом проб.

6	Найти все возможные значения модуля шифрования меньшие 20.
7	Выполнить пошагово алгоритм Эвклида для аргументов 1234 и 54.
8	Определить достаточное число ключей для реализации алгоритма ТНДШ для возможности шифрования 5 сообщений, если в каждом сообщении может быть до 200 двоичных символов.
9	Вычислить функцию Эйлера для следующих аргументов: 323, 1013, 10403.
10	Произвести шифрования сообщения по алгоритму РША. Вычислить криптограмму из сообщения M=3. Открытый ключ: K=5, N=187.
11	Определить количество единиц на периоде выходной последовательности ЛРР заданного следующим полиномом: h(x)=x^4+x+1.
12	Определить достаточное число ключей для реализации алгоритма ТНДШ для возможности шифрования 10 сообщений, если в каждом сообщении может быть до 100 двоичных символов.
13	Определить количество единиц на периоде выходной последовательности ЛРР заданного следующим полиномом: h(x)=x^5+x+1.
14	Сформировать цифровую подпись для сообщения M=7, если используется алгоритм РША (без хеширования). Секретный ключ пользователя: k=3, N=77.
15	Определить верхнюю границу эффективного объёма ключа при двухкратном шифровании на разных ключах на алгоритме DES.
16	Найти секретный ключ для алгоритма РША, если открытый ключ: K=7, N=24.
17	Оценить сверху максимально возможный объём подписанного сообщения, если в качестве алгоритма цифровой подписи используется алгоритм Эль-Гамаля (без хеширования и без разбиения сообщения на блоки) с параметрами: a=31, p=9901.
18	Найти значения следующих выражений: 2^12 mod11, 2^22 mod35, 4*3^(-1)mod5.
19	Выполнить по шагам вычисление 2^11 mod 7 быстрым алгоритмом возведения в степень.
20	Выполнить пошагово алгоритм разложения на множители Ферма для числа 253.
21	Выполнить по шагам вычисление 3^8 mod 7 быстрым алгоритмом возведения в степень.
22	Выполнить пошагово тест Миллера для числа 561 по основанию 2.
23	Найти секретный ключ для алгоритма РША, если открытый ключ: K=7, N=24.
24	Определить верхнюю границу эффективного объёма ключа при двухкратном шифровании на разных ключах на алгоритме DES.
25	Выполнить пошагово тест Миллера для числа 25 по основанию 7.
26	Найти секретный ключ для алгоритма РША, если открытый ключ: K=7, N=20.
27	Определить расстояние единственности для криптограммы сообщения с энтропией равной 2, если шифрование выполнено российским стандартом шифрования ГОСТ 28147-89.
28	Определить количество ключей в системе шифрования методом простой замены для текста на английском языке.
29	Определить расстояние единственности для криптограммы сообщения с энтропией равной 1,5, если шифрование выполнено российским стандартом шифрования AES.
30	Определить расстояние единственности для криптограммы сообщения с энтропией равной 2,5, если шифрование выполнено российским стандартом шифрования ГОСТ Р 34.12-2015

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

4.3.Развернутые критерии выставления оценки

Таблица 5

Тип вопроса	**Показатели оценки**			
	5	**4**	**3**	**2**

Теорети-ческие 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
Практи-ческие вопросы	задача решена без ошибок, студент может дать все необходимые пояснения к решению, сделать выводы	задача решена без ошибок, но студент не может пояснить ход решения и сделать необходимые выводы	задача решена с одной ошибкой, при ответе на вопрос ошибка замечена и исправлена самостоятельно	задача не решена или решена с двумя и более ошибками, пояснения к ходу решения недостаточны
Дополни-тельные 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	недоста-точный

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

Собеседование – это средство контроля, организованное как специальная беседа преподавателя со студентом на темы, связанные с изучаемой дисциплиной, и рассчитанное на выявление объема знаний студента по определенному разделу, теме, проблеме и т.п., соответствующих освоению компетенций, предусмотренных рабочей программой дисциплины.

Проблематика, выносимая на собеседование, определяется преподавателем в заданиях для самостоятельной работы студента, а также на семинарских и практических занятиях. В ходе собеседования студент должен уметь обсудить с преподавателем соответствующую проблематику на уровне диалога и показать установ

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», «незачтено».

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».