

**Санкт-Петербургский филиал федерального государственного
автономного образовательного учреждения высшего образования
«Национальный исследовательский университет
"Высшая школа экономики"»**

Факультет Санкт-Петербургская школа
физико-математических и компьютерных наук
Департамент информатики

**Рабочая программа дисциплины
Криптографические протоколы**

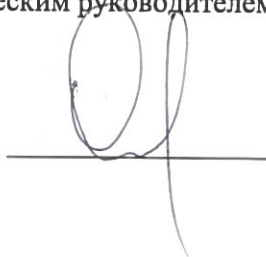
для образовательной программы «Прикладная математика и информатика»
направления подготовки 01.03.02 «Прикладная математика и информатика»
уровень бакалавриат

Разработчик: Афанасьева Александра Валентиновна, avafanaseva@hse.ru

Утверждена Академическим руководителем образовательной программы

«31» августа 2018 г.

А.В. Омельченко



Санкт-Петербург, 2018

Настоящая программа не может быть использована другими подразделениями университета и другими вузами без разрешения подразделения-разработчика программы.

1. Область применения и нормативные ссылки

Настоящая программа учебной дисциплины устанавливает требования к образовательным результатам и определяет содержание и виды учебных занятий и отчетности.

Программа предназначена для преподавателей, ведущих дисциплину «Криптографические протоколы», учебных ассистентов и студентов направления 01.03.02 «Прикладная математика и информатика» подготовки бакалавра, обучающихся по бакалаврской программе «Прикладная математика и информатика» и изучающих дисциплину «Криптографические протоколы».

Рабочая программа дисциплины разработана в соответствии с:

- Образовательным стандартом НИУ ВШЭ по направлению подготовки 01.03.02 «Прикладная математика и информатика» (уровень бакалавриата), утвержденным ученым советом Национального исследовательского университета «Высшая школа экономики», протокол от 03.03.2017 №02.
- Основной профессиональной образовательной программой «Прикладная математика и информатика» направления подготовки 01.03.02 «Прикладная математика и информатика»;
- Объединенным учебным планом университета по образовательной программе «Прикладная математика и информатика», утвержденным в 2018 г.

2. Цели освоения дисциплины

Целями освоения 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.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины студент должен:

- Знать основные понятия и факты криптологии, такие, как алгоритмы симметричного и асимметричного шифрования; классические и специальные определения криптографической стойкости и анонимности; правила управления ключами; основные протоколы классической и постквантовой криптографии.
- Уметь оценивать и доказывать стойкость криптографических протоколов, выбирать криптографические примитивы и их параметры в зависимости от реализуемого протокола; обеспечивать контроль целостности информации.
- Иметь навыки (приобрести опыт) построения и анализа криптографических протоколов, управления ключами.

В результате освоения дисциплины студент осваивает следующие компетенции:

Компетенция	Код по ОС НИУ ВШЭ	Уровень формирования компетенции	Дескрипторы – основные признаки освоения (показатели достижения результата)	Формы и методы обучения, способствующие формированию и развитию компетенции	Форма контроля уровня сформированности и компетенции
Способен решать проблемы в профессиональной деятельности на основе анализа и синтеза	УК-3	РБ СД МЦ	Выявляет достоверные источники информации. Обработывает, анализирует и синтезирует информацию. Использует криптографические методы для решения практических задач.	Лекции, подготовка к практическим занятиям, работа на практических занятиях, самостоятельная работа	Письменные домашние задания, устный экзамен

Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности	ОПК-1	РБ СД МЦ	Знает понятие криптографической стойкости шифра. Оценивает сложность алгоритмов для взлома шифра. Разрабатывает программы для шифрования и дешифровки данных.	Лекции, подготовка к практическим занятиям, работа на практических занятиях, самостоятельная работа	Письменные домашние задания, устный экзамен
Способен применять и модифицировать математические модели для решения задач в области профессиональной деятельности	ОПК-3	РБ СД МЦ	Знает основные криптографические алгоритмы. Модифицирует и реализует данные алгоритмы. Выбирает наиболее подходящие алгоритмы для решения конкретной прикладной задачи.	Лекции, подготовка к практическим занятиям, работа на практических занятиях, самостоятельная работа	Письменные домашние задания, устный экзамен
Способен разрабатывать и реализовывать в виде программного модуля алгоритм решения поставленной теоретической или прикладной задачи на основе математической модели	ПК-2	РБ СД МЦ	Знает основные криптографические протоколы. Разрабатывает программы, основанные на протоколах цифровой идентификации и управления ключами. Владеет навыками работы с различными протоколами разделения секрета.	Лекции, подготовка к практическим занятиям, работа на практических занятиях, самостоятельная работа	Письменные домашние задания, устный экзамен
Способен анализировать, писать и редактировать академические и технические тексты на русском и иностранном языках для решения задач профессиональной и научной деятельности в области математики и компьютерных наук	ПК-4	РБ СД МЦ	Знает принципы написания сопровождающей технической документации. Анализирует имеющуюся техническую документацию к программам на русском и английском языках. Создаёт документацию и анализа академических текстов для решения задач.	Лекции, подготовка к практическим занятиям, работа на практических занятиях, самостоятельная работа	Письменные домашние задания, устный экзамен
Способен строить профессиональную деятельность на основе правовых, профессиональных и этических норм и обязанностей,	ПК-6	РБ СД	Знает основные положения об охране интеллектуальных прав и защите информации. Создаёт сопроводительную документацию по	Лекции, подготовка к практическим занятиям, работа на практических занятиях, самостоятельная	Письменные домашние задания, устный экзамен

выполнять технологические требования и нормативы		МЦ	результатам разработки ПО. Владеет навыками составления технической документации.	работа	
--	--	----	---	--------	--

4. Место дисциплины в структуре образовательной программы

Для образовательной программы «Прикладная математика и информатика» направления подготовки 01.03.02 «Прикладная математика и информатика» настоящая дисциплина относится к дисциплинам по выбору блока дисциплин.

Для освоения дисциплины необходимы компетенции, полученные в ходе изучения дисциплин:

- Теория информации.

5. Тематический план учебной дисциплины

Курс рассчитан на 44 часа аудиторной нагрузки, из них 22 часа лекций и 22 часов практических занятий, общим объемом 3 зачетных единиц (114 часов).

№	Название раздела	Всего часов	Аудиторные часы			Самостоятельная работа
			Лекции	Семинары	Практические занятия	
1	Криптографические алгоритмы	57	11	0	11	35
2	Криптографические протоколы	57	11	0	11	35
ИТОГО		114	22	0	22	70

6. Содержание дисциплины

<u>Раздел 1</u> Криптографические алгоритмы	
Тема 1	Основные понятия криптографии. Предмет и задачи. Определение шифра, понятие стойкости, предположения об исходных условиях криптоанализа, симметричные и асимметричные криптосистемы, хэш-функции, криптографические протоколы. История криптографии. Принцип Керкгоффса. Понятие абсолютной стойкости или теоретико-информационной стойкости.
Тема 2	Симметричные криптосистемы. Потокосые шифры. Одноразовый блокнот. Понятие псевдослучайности. Требования к потокосым шифрам: Постулаты Голomba, профиль линейной сложности. Методы построения больших периодов в поточных шифрах. Статистические тесты. Применение к известным генераторам. Понятие псевдослучайного генератора (PRG) и его криптографическая стойкость. Семантическая стойкости криптосистемы. Блочные шифры. Определение блочного шифра. Требования к блочным шифрам. Различие понятий PRP и PRF. Определение стойкости. Способы построение блочных шифров: подстановки, перестановки, сети Фейстеля. Алгоритм DES. Режимы использования блочных

	шифров (“электронная кодовая книга”, режимы с зацеплением, режимы использования блочных шифров для получения поточных шифров). Детерминированные и недетерминированные алгоритмы шифрования. Влияние случайности на стойкость. Слабости блочных шифров.
Тема 3	Контроль целостности. MAC. Определение, модель безопасности. Построение на базе Блочных шифров: VCB-MAC, NMAC, PMAC. Хэш-функции. Стойкость к коллизиям. Требования к хэш-функциям. Парадокс дней рождения. Примеры хэш-функций. HMAC. CCA модель атак и аутентифицированное шифрование. Способы построения AE. Стандарты.
Тема 4	Основные алгоритмы с открытым ключом. Схема RSA. Атаки на RSA. Базовые задачи, допущение Диффи и Хелмана. Возможность реализации систем на мультипликативной группе точек эллиптических кривых. Схема шифрования ElGamal. Базовые задачи, допущение Диффи и Хелмана. Схема шифрования Меркла-Хелмана. Электронная цифровая подпись. Основные понятия, требования. Определение безопасности.
<u>Раздел 2</u> Криптографические протоколы	
Тема 1	Управление ключами. Попарные ключи. Использование мастер-ключей. Система Диффи и Хелмана. Человек посередине. Протоколы обмена ключами. С сервером, без сервера. Известные атаки на протоколы обмена ключами. К-надежные схемы распределения ключей. Протоколы разделения секрета. Пороговая криптография.
Тема 2	Протоколы цифровых денег и электронного голосования. Протоколы электронного голосования. Криптографическая реализация. Слепая подпись. Требования безопасности. Защищенные распределенные вычисления. Доказательства с нулевым разглашением. Примеры систем.
Тема 3	Протоколы идентификации + личностная криптография. Схема идентификации Schnorr – Shamir. Схема идентификации Feige – Fiat – Shamir. Инфраструктура открытых ключей и альтернативные подходы(ID-based распределенные системы).
Тема 4	Пост-квантовая криптография. Понятия квантовых вычислений. Построение криптосистем на доказано сложных задачах. Линейные коды. Способы задания. Декодирование линейных кодов как «трудная» задача. Декодирование линейных кодов как «простая» задача. NP- полные задачи кодирования. Системы Макэлиса и Нидерайтора.

7.Оценочные средства

7.1. Формы контроля знаний студентов

Тип контроля	Форма контроля	4 год	Параметры
		3 модуль	
Текущий	Домашнее задание №1	*	Письменное домашнее задание

	Домашнее задание №2	*	Письменное домашнее задание
	Домашнее задание №3	*	Письменное домашнее задание
	Домашнее задание №4	*	Письменное домашнее задание
Итоговый	Устный экзамен	*	Экзамен в устной форме

7.2. Критерии и шкалы оценки, примеры заданий

Текущий контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств.

ДОМАШНЕЕ ЗАДАНИЕ №1

Домашнее задание №1 выдается студентам в одном варианте и состоит из 3 задач. Каждой задаче присвоен свой балл. Срок выполнения домашнего задания - 2 недели. Форма представления обучающимися домашнего задания - представленные в письменном виде решения задач.

Пример домашнего задания №1:

Задача 1.[4 балла] Оценить теоретически количество зашифрованного текста (в символах) для успешного частотного криптоанализа и подтвердить результаты экспериментально, если известно, что открытый текст – это осмысленный текст на русском языке и была использована следующая система шифрования:

- 1) Шифр Цезаря;
- 2) Аффинный шифр;
- 3) Шифр Вижинера с известной длиной ключа (показать зависимость от длины ключа);
- 4) Шифр Вижинера с неизвестной длиной ключа (показать зависимость от длины ключа).

Задача 2.[4 балла] Простым перестановочным шифром зашифрован некий текст, при этом известно, что в качестве открытого текста использован палиндром, в котором все пробелы и знаки препинания опущены. В результате шифрования получен следующий текст: МТИССЛАИЛПНАОЛМУИЛОПИТУ
Необходимо:

- 1) Расшифровать текст,
- 2) Оценить, насколько можно уменьшить сложность перебора, используя информацию об исходном сообщении;
- 3) При программной реализации минимизировать количество возвращаемых вариантов ответа.
- 4) Позволяет ли успешный криптоанализ данного сообщения раскрыть ключ шифрования?

Задача 3.[2 балла] Шифром простой замены зашифровано некоторое стихотворение, при этом сохранены все пробелы и знаки препинания, одинаковые символы заменены одинаковыми, а различные - различными. В результате шифрования получился следующий текст:

Э рсдх ыгсг, фрьбя сзя тцорт срэдт
Юрь нфурсау уцир нэръ, мрьбя
Нрусиь рнмясяэуцэяуц нурэрт,

Нурэрт оячолжяуц ьрорья.

- 1) Расшифровать текст,
- 2) Позволяет ли успешный криптоанализ данного сообщения раскрыть ключ шифрования?

Критерии оценивания и шкала оценки домашнего задания №1

Оценка	Критерии выставления оценки
«Отлично» (8-10)	Решено задач на 8 или более баллов
«Хорошо» (6-7)	Решено задач на 6-7 баллов
«Удовлетворительно» (4-5)	Решено задач на 4-5 баллов
«Неудовлетворительно» (0-3)	Решено задач на менее чем 4 балла

ДОМАШНЕЕ ЗАДАНИЕ №2

Домашнее задание №2 выдается студентам в одном варианте и состоит из 4 задач. Каждой задаче присвоен свой балл. Срок выполнения домашнего задания - 2 недели. Форма представления обучающимися домашнего задания - представленные в письменном виде решения задач.

Пример домашнего задания №2:

Задача 1. [6 баллов]

Рассмотреть генератор псевдослучайной последовательности. Вначале выбираются два больших простых числа p и q . Числа p и q должны быть оба сравнимы с 3 по модулю 4. Далее вычисляется число $M = p * q$, называемое целым числом Блюма. Затем выбирается другое случайное целое число x , взаимно простое с M . Вычисляем $cx_0 = x^2 \bmod M$. x_0 называется стартовым числом генератора.

На каждом n -м шаге работы генератора вычисляется $x_n = x_{n-1}^2 \bmod M$. Результатом n -го шага является бит чётности числа x_n , то есть сумма по модулю 2 единиц в двоичном представлении элемента.

Для данного генератора оценить статистические свойства при помощи следующих тестов:

- 1) (monobit test) равно ли количество нулей и единиц;
- 2) (two-bit test) равно ли количество 00, 01, 10 и 11;
- 3) (poker test) равно ли количество разных последовательностей длины m ;
- 4) (runs test) подходящее ли количество последовательностей идущих подряд нулей и единиц той или иной длины;
- 5) (autocorrelation test) одинаковая ли автокорреляция на разных сдвигах;

Построить для генератора профиль линейной сложности

Задача 2. [2 балла]

Пусть $G: K \rightarrow \{0,1\}^n$ псевдослучайный генератор, про который известно, что для него по значениям последних $n/2$ бит можно построить первые $n/2$ бит.

Является ли данный генератор G предсказуемым для какого-либо $i \in \{0, n-1\}$?

Задача 3. [3 балла]

Доказать, что одноразовый блокнот является семантически стойким алгоритмом шифрования.

Задача 4. [6 баллов]

Пусть $G: K \rightarrow \{0,1\}^n$ криптографически стойкий псевдослучайный генератор (PRG), тогда потоковый шифр, основанный на нем, будет семантически стойким.

Чтобы подтвердить это утверждение докажите, что для любого атакующего шифр алгоритма A , существует алгоритм B для функции G , такой что:

$$Adv_{SS}[A, E] \leq 2Adv_{PRG}[B, G]$$

Критерии оценивания и шкала оценки домашнего задания №2

Оценка	Критерии выставления оценки
«Отлично» (8-10)	Решено задач на 13 или более баллов
«Хорошо» (6-7)	Решено задач на 10-12 баллов
«Удовлетворительно» (4-5)	Решено задач на 7-9 баллов
«Неудовлетворительно» (0-3)	Решено задач на менее чем 7 баллов

ДОМАШНЕЕ ЗАДАНИЕ №3

Домашнее задание №3 выдается студентам в одном варианте и состоит из 5 задач. Каждой задаче присвоен свой балл. Срок выполнения домашнего задания - 2 недели. Форма представления обучающимися домашнего задания - представленные в письменном виде решения задач.

Пример домашнего задания №3:**Задача 1. [1,5 балла]**

Рассмотрим MAC Картера-Вегмана (Carter---Wegman MAC) $I_{CW} = (S_{CW}, V_{CW})$, который строится на основе стойкого одноразового MAC $I=(S,V)$ и стойкой PRF функции $F(k,m)$. Проверочное значение tag формируется по правилу:

$$tag = S_{CW}((k_1, k_2), m) = (r, F(k_1, r) S(k_2, m)), \quad r \leftarrow \{0,1\}^n$$

Построить функцию верификации для проверки сообщения $V_{CW}(m, tag)$.

Задача 2. [5 баллов]

Предложить хэш-функцию, стойкую к коллизиям $h(H,m)$, на основе стойкого блочного шифра $E: K \times \{0,1\}^n \rightarrow \{0,1\}^n$. Предложенная хэш-функция должна отображать $h: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n$.

Какое максимальное количество различных конструкций с данными свойствами вы можете предложить?

Задача 3. [3 балла]

Будет ли стойкой к коллизиям хэш-функция, на основе стойкого блочного шифра $E: K \times \{0,1\}^n \rightarrow \{0,1\}^n$, следующего вида: $h(H,m) = E(m,H) \oplus m$? Ответ обосновать.

Задача 4. [2 балла]

Оценить во сколько раз увеличится длина передаваемого сообщения в 1 байт, если оно зашифровано:

- алгоритмом шифрования AES в режиме CBC со случайным IV.
- алгоритмом шифрования AES в режиме CTR.
- алгоритмом шифрования AES в режиме OFB со случайным IV.
- алгоритмом шифрования 3DES в режиме CBC со случайным IV.

Задача 5. [3 балла]

Пусть заданы множества $X=\{0,1\}$ и $K=\{0,1\}$.

Определим псевдослучайную перестановку PRP следующим образом: $E(k,x) = x \oplus k$.

Будет ли эта перестановка криптографически стойкой?

Будет ли предложенная функция псевдослучайной функцией PRF?

Критерии оценивания и шкала оценки домашнего задания №3

Оценка	Критерии выставления оценки
«Отлично» (8-10)	Решено задач на 12 или более баллов
«Хорошо» (6-7)	Решено задач на 9-11 баллов
«Удовлетворительно» (4-5)	Решено задач на 6-8 баллов
«Неудовлетворительно» (0-3)	Решено задач на менее чем 6 баллов

ДОМАШНЕЕ ЗАДАНИЕ №4

Домашнее задание №4 выдается студентам в пяти вариантах и содержит всего одно задание. Вариант студенты могут выбирать самостоятельно. Оценивается степень выполнения задания. Срок выполнения домашнего задания - 2 недели. Форма представления обучающимися домашнего задания - представленные в письменном виде решения задач.

Пример домашнего задания №4:

Вариант 1.

Изучить протокол пороговой подписи, предложенный в статье Victor Shoup, «Practical Threshold Signatures» Дополнить процедурой выдачи новой проекции ключа без дилера.

Вариант 2.

Изучить протокол пороговой подписи, предложенный в статье Rosario Gennaro, Shai Halevi, Hugo Krawczyk, Tal Rabin, «Threshold RSA for Dynamic and Ad-Hoc Groups».

Дополнить протокол процедурой выдачи новой проекции ключа без дилера.

Вариант 3.

Изучить протокол пороговой подписи, предложенный в статье АД Фомина, «Распределенная подпись RSA».

Дополнить процедурой обновления проекций участников без замены общего секрета.

Вариант 4.

Изучить протокол пороговой подписи, предложенный в статье Jiejun Kong ; Z. Petros ; Haiyun Luo ; Songwu Lu ; Lixia Zhang, “ Providing robust and ubiquitous security support for mobile ad-hoc networks”

Оценить количество разглашаемой информации при постановке подписи. Предложить модификацию, позволяющую обновлять проекции секретного ключа. Оценить возможность и невозможность утечки при этой процедуре.

Вариант 5.

Предложить пороговую схему k из n реализации российского стандарта ЭЦП.

Критерии оценивания и шкала оценки домашнего задания №4

Оценка	Критерии выставления оценки
«Отлично» (8-10)	Студент полностью разобрался с предложенной статьей. Предложено полное решение поставленной задачи, приведено обоснование криптостойкости нового протокола.
«Хорошо» (6-7)	Студент полностью разобрался с предложенной статьей. Модификация протокола или доказательство содержит ошибки.
«Удовлетворительно» (4-5)	Студент полностью разобрался с предложенной статьей. Но не смог решить поставленную задачу или решил некорректно.
«Неудовлетворительно» (0-3)	Возникли сложности с пониманием предложенной статьи.

7.2.2. Итоговый контроль по дисциплине

Проверка качества освоения дисциплины производится в форме устного экзамена.

УСТНЫЙ ЭКЗАМЕН

Устный экзамен проводится в форме ответов на вопросы экзаменационного билета. Экзаменационный билет формируется из двух вопросов из перечня вопросов к экзамену. На подготовку ответа выделяется 40 минут.

Примерный перечень вопросов к экзамену:

1. Предмет и задачи. Определение шифра, понятие стойкости.
2. Предположения об исходных условиях криптоанализа
3. Симметричные и асимметричные криптосистемы, хэш-функции, криптографические протоколы.
4. История криптографии. Криптография древности, частотный криптоанализ.
5. Криптография нового времени.
6. Криптография XX века. Принцип Керкгоффса.
7. Понятие абсолютной стойкости или теоретико-информационной стойкости. Одноразовый блокнот.
8. Понятие псевдослучайности.
9. Поточные шифры. Синхронные и самосинхронизирующиеся шифры
10. Требования к поточным шифрам: Постулаты Голомба, профиль линейной сложности.
11. Методы построения больших периодов в поточных шифрах. Регистры сдвигов с линейной обратной связью.
12. Статистические тесты.
13. Семантическая стойкость. CPA модель атаки.
14. Требования к блочным шифрам. PRP и PRF.
15. Способы построения блочных шифров: подстановки, перестановки, сети Фейстеля.
16. Примеры симметричных шифров: DES, AES.

17. Подходы к криптоанализу: линейный, дифференциальный, «встреча посередине».
18. Режимы использования блочных шифров («электронная кодовая книга», режимы с зацеплением, режимы использования блочных шифров для получения поточных шифров).
19. Детерминированные и недетерминированные алгоритмы шифрования.
20. Влияние случайности на стойкость. Слабости блочных шифров.
21. Контроль целостности. MAC. Определение, модель безопасности. Построение на базе Блочных шифров.
22. HMAC. Хэш-функции. Требования к хэш-функциям.
23. Аутентифицированное шифрование.
24. ССА модель атаки. Примеры активных атак.
25. Понятие алгоритма с открытым ключом.
26. Схема RSA. Атаки на RSA.
27. Схема шифрования ElGamal. Базовые задачи, допущение Диффи и Хелмана.
28. Управление ключами. Групповые ключи. Парные ключи. Использование мастер-ключей.
29. Протоколы обмена ключами. С сервером, без сервера.
30. Известные атаки на протоколы обмена ключами.
31. К-надежные схемы распределения ключей
32. Протоколы разделения секрета.
33. Пороговая криптография.
34. Протоколы цифровых денег и электронного голосования.
35. Слепая подпись.
36. Схема идентификации Schnorr – Shamir.
37. Схема идентификации Feige – Fiat – Shamir.
38. Инфраструктура открытых ключей и альтернативные подходы(ID-based распределенные системы).
39. Понятие анонимности пользователей. Постановки задачи. PIR (протоколы конфиденциального получения информации).
40. Понятия квантовых вычислений.
41. Построение криптосистем на доказано сложных задачах. Линейные коды. Способы задания.
42. Декодирование линейных кодов как «трудная» задача. Декодирование линейных кодов как «простая» задача.
43. Системы Макэлиса и Нидерайтора.

Критерии оценивания и шкала оценки устного экзамена

Оценка	Критерии выставления оценки
«Отлично» (8-10)	Даны развернутые ответы на поставленные вопросы. Материал изложен последовательно. Имеются логичные и аргументированные выводы.
«Хорошо» (6-7)	Даны развернутые ответы на поставленные вопросы. Материал изложен в целом последовательно. Имеются логичные и аргументированные выводы.

«Удовлетворительно» (4-5)	Ответы на вопросы не являются полными. Материал изложен непоследовательно. Выводы не аргументированы.
«Неудовлетворительно» (0-3)	Ответы на вопросы являются неверными. Материал изложен непоследовательно. Отсутствуют выводы.

7.3. Порядок формирования оценок по дисциплине

Результирующая оценка за дисциплину рассчитывается следующим образом:

$$O_{\text{Результирующая}} = 0,5 * O_{\text{накопленная}} + 0,5 * O_{\text{экзамен}}$$

где $O_{\text{накопленная}}$ рассчитывается как взвешенная сумма всех форм текущего контроля.

$$O_{\text{накопленная}} = 0,25 * O_{\text{д/з1}} + 0,25 * O_{\text{д/з2}} + 0,25 * O_{\text{д/з3}} + 0,25 * O_{\text{д/з4}}$$

Действует следующий способ округления накопленной оценки текущего контроля: при значениях от 0,1 до 0,4 оценка округляется в меньшую сторону, от 0,5 до 0,9 – в большую.

Результирующая оценка округляется в большую сторону.

На экзамене студенту не предоставляется возможность получить дополнительный балл для компенсации оценки за текущий контроль.

8. Образовательные технологии

Основными образовательными технологиями являются: интерактивные лекции, работа в группах на практических занятиях.

9. Учебно-методическое и информационное обеспечение дисциплины

9.1 Основная литература

1. Algebraic Geometry for Coding Theory and Cryptography: IPAM, Los Angeles, CA, February 2016 / Howe, Everett W; Lauter, Kristin E; Walker, Judy L. Springer. 2017
2. Фомичев В.М. Криптографические методы защиты информации В 2 Ч. ЧАСТЬ 1. Математические аспекты. Учебник для академического бакалавриата/В.М.Фомичев, Д.А.Мельникова; под ред. В.М.Фомичева.- М.: Издательство Юрайт, 2018 - 209 с.

9.2 Дополнительная литература

1. Фомичев В.М. Криптографические методы защиты информации В 2 Ч. ЧАСТЬ 2. Системные и прикладные аспекты. Учебник для академического бакалавриата/В.М.Фомичев, Д.А.Мельникова; под ред. В.М.Фомичева.- М.: Издательство Юрайт, 2018 - 245 с.
2. Understanding Cryptography / Christof Paar; Jan Pelzl; Nugent. Springer Berlin Heidelberg. 2010
3. Cryptography / Rubinstein-Salzedo; Amzad. Springer International Publishing. 2018

10. Рекомендации для самостоятельной работы студентов.

Самостоятельная работа может рассматриваться как организационная форма обучения - система педагогических условий, обеспечивающих управление учебной деятельностью по освоению знаний и умений в области учебной деятельности без посторонней помощи. Студенту нужно четко понимать, что самостоятельная работа – не просто обязательное, а необходимое условие для получения знаний по дисциплине и развитию компетенций, необходимых в будущей профессиональной деятельности.

Самостоятельная работа проводится с целью:

- систематизации и закрепления полученных на лекциях теоретических знаний;
- углубления и расширения теоретических знаний;
- формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развития познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- формирования практических (общеучебных и профессиональных) умений и навыков;
- развития исследовательских умений;
- получения навыков эффективной самостоятельной профессиональной (практической и научно-теоретической) деятельности.

В учебном процессе выделяют два вида самостоятельной работы:

- аудиторная;
- внеаудиторная.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа - планируемая учебная работа студентов, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Самостоятельная работа, не предусмотренная программой учебной дисциплины, раскрывающей и конкретизирующей ее содержание, осуществляется студентом инициативно, с целью реализации собственных учебных и научных интересов.

Для более эффективного выполнения самостоятельной работы по дисциплине преподаватель рекомендует источники для работы, характеризует наиболее рациональную методику самостоятельной работы, демонстрирует ранее выполненные студентами работы и т. п.

Виды заданий для внеаудиторной самостоятельной работы, их содержание и характер могут иметь вариативный и дифференцированный характер, учитывать индивидуальные особенности студента.

Самостоятельная работа может осуществляться индивидуально или группами студентов online и на занятиях в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности.

Контроль результатов внеаудиторной самостоятельной работы осуществляется в пределах времени, отведенного на обязательные учебные занятия по дисциплине на практических занятиях.

11. Материально-техническое обеспечение дисциплины и информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения информационных справочных систем (при необходимости).

Для проведения всех занятий используется проектор и компьютер для проекции слайдов. Для самостоятельной работы необходимо следующее ПО: GNU C++, Oracle Java, Python.

12. Особенности организации обучения для лиц с ограниченными возможностями здоровья

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться следующие варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

1) для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат);

индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.

2) для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

3) для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.