МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета

_____ Нестеров П.Н.

20 июня 2023 г.

Рабочая программа дисциплины

Сложностная криптография

Направление подготовки (специальности)
10.04.01 Информационная безопасность

Направленность (профиль)
«Управление информационной безопасностью»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 14 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

Ярославль

1. Цели освоения дисциплины

Целью освоения дисциплины «Сложностная криптография» является приобретение обучающимися теоретических знаний в области современной сложностной криптографии и практических навыков анализа криптографических примитивов с помощью математического аппарата сложностной криптографии.

Дисциплина обеспечивает приобретение передовых знаний в одной из наиболее динамично развивающихся областей современной криптографии.

2. Место дисциплины в структуре образовательной программы

Данная дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений.

Для освоения данной дисциплины обучающиеся должны владеть основными понятиями теории алгоритмов, математическим аппаратом теории вероятностей и математической статистики, знать основные методы криптографической защиты информации.

Для успешного освоения дисциплины «Сложностная криптография» ей должны предшествовать следующие дисциплины:

«Теоретико-числовые методы в криптографии»;

«Сложность вычислений»;

«Теория алгоритмов».

Дисциплина «Сложностная криптография» является предшествующей для прохождения производственной и преддипломной практики и итоговой государственной аттестации.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Общепрофессиональные компетенции		
ПК-1 Способен разрабатывать математические модели систем обеспечения информационной безопасности, математически	И-ПК-1.1 Знает основные математические модели систем обеспечения информационной безопасности и математические методы обеспечения	Знать: - историю, этапы развития и перспективы развития сложностной криптографии; - основные методы анализа криптографических примитивов с использованием математического аппарата сложностной криптографии.

доказывать их соответствие выбранным политикам безопасности	И-ПК-1.2 Владеет навыками разработки и реализации алгоритмов решения типовых профессиональных задач на языках высокого уровня	Владеть навыками: - использования современных сред разработки программного обеспечения, систем контроля версий; - разработки алгоритмов защиты информации на основе сложностной криптографии.
ПК-2 Способен анализировать математические модели систем обеспечения информационной безопасности, а также проводить тестирование средств защиты информации на соответствие этим моделям	И-ПК-2.1 Знает основные виды атак на информационную инфраструктуру и математические методы противодействия им	Знать: - основные виды атак на криптографические примитивы, разработанные на основе сложностной криптографии; - методы анализа защищенности криптографических примитивов, созданных на основе сложностной криптографии
	И-ПК-2.1 Умеет разрабатывать и применять математические методы противодействия атакам на информационные системы и инфраструктуру	Уметь: - применять математического аппарата сложностной криптографии для анализа криптографических примитивов.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 5 зачетных единиц, 180 акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам)
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
1	Односторонние функции: Односторонние в наихудших случаях функции. Сильные и слабые односторонние	3	4	2		1		8	Задания для самостоятельной работы

	функции. Вопросы длин входов. Эквивалентность существования сильной и слабой односторонних функций								
2	Семейство односторонних функций. Трудный бит: Семейство односторонних функций. Универсальная односторонняя функция. Трудный бит	3	4	2		1		8	Задания для самостоятельной работы
3	Генераторы псевдослучайных чисел: Вычислительная неразличимость. Генераторы псевдослучайных чисел. Протоколы с секретным ключом	3	4	6		1		10	Задания для самостоятельной работы
4	Псевдослучайные функции: Вычислительная неразличимость полиномиального числа образцов. Ансамбли функций. Конструкция ансамбля псевдослучайных функций	3	6	6		1		10	Задания для самостоятельной работы
5	Привязка к биту: Неинтерактивные протоколы. Интерактивные протоколы	3	2	2		1		8	Задания для самостоятельной работы
6	Доказательства с нулевым разглашением: Интерактивные системы доказательства. Совершенно нулевое разглашение. Вычислительно нулевое разглашение. Доказательства с нулевым разглашением для NP	3	4	4		1		8	Задания для самостоятельной работы
7	Шифрование с открытым ключом: Семейство односторонних перестановок с секретом. Шифрование с открытым	3	2	4		1		8	Задания для самостоятельной работы

	ключом								
8	Цифровые подписи: Цифровая подпись одного бита. Цифровая подпись фиксированного числа битов. Цифровая подпись сообщения произвольной длины. Построение СТОК и СТОЗ. Протокол подписи сообщений произвольной длины на основе односторонней функции. Протокол подписи произвольного количества сообщений произвольной длины	3	6	6		1		12	Задания для самостоятельной работы
						2	0,5	33,5	Экзамен
	ИТОГО	**180**	**32**	**32**		**10**	**0,5**	**105,5**	

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Проблемная лекция – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов, авторские комментарии, связанные с различными моделями интерпретации изучаемого материала. Проблемная лекция начинается с вопросов, с постановки проблемы, которую в ходе изложения материала необходимо решить. В лекции сочетаются проблемные и информационные начала. При этом процесс познания студентов в сотрудничестве и диалоге с преподавателем приближается к поисковой, исследовательской деятельности. Содержание проблемы раскрывается путем организации поиска ее решения или суммирования и анализа традиционных и современных точек зрения.

Лекция с заранее запланированными ошибками – рассчитана на стимулирование студентов к постоянному контролю предлагаемой информации (поиск ошибки: содержательной, методологической, методической). Используется для развития у студентов умения оперативно анализировать профессиональные ситуации, выступать в роли экспертов, оппонентов, рецензентов, вычленять неверную или неточную информацию. Подготовка преподавателя к лекции состоит в том, чтобы заложить в ее содержание определенное количество ошибок содержательного или методического характера. Лектор строит изложение таким образом, чтобы ошибки были тщательно «замаскированы» и их не так-то

легко было заметить слушателям. Задача слушателей состоит в том, чтобы по ходу лекции отмечать в конспекте замеченные ошибки, чтобы назвать их в конце лекции. На разбор ошибок отводится 10-15 минут.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса используются:

для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- издательская система LaTex;
- Adobe Acrobat Reader;

при проведении практических занятий используется программное обеспечение

- Microsoft Visual Studio.

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

Для поиска учебной литературы библиотеки ЯрГУ используется автоматизированная библиотечно-информационная система «БУКИ-NEXT» http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php.

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

1. *Верещагин Н.К.* Лекции по математической криптографии / Н.К. Верещагин – 2015, 169 с. (https://www.studmed.ru/vereschagin-n-k-lekcii-po-matematicheskoy-kriptografii_ecfb68dbe76.html).

б) дополнительная литература

1. *Goldreich O.* Foundations of Cryptography Basic Tools / O. Goldreich – 2004, 372 с.

в) ресурсы сети «Интернет» (при необходимости)

1. Мультимедийные материалы Computer Science клуба (Санкт-Петербург). Курс «Сложностная криптография», 2008, читает доктор физико-математических наук, ведущий научный сотрудник лаборатории математической логики ПОМИ РАН, заместитель заведующего кафедрой МиИТ СПбАУ РАН, Э. А. Гирш (http://compsciclub.ru/courses/complexitycrypto/2008-spring/?tab=classes).

2. Мультимедийные материалы Computer Science клуба (Санкт-Петербург). Курс «Сложность вычислений и основы криптографии», 2012, читает доктор физико-математических наук, ведущий научный сотрудник лаборатории математической логики ПОМИ РАН, заместитель заведующего кафедрой МиИТ СПбАУ РАН, Э. А. Гирш (http://compsciclub.ru/courses/cryptography/2012-spring/?tab=classes).

3. Мультимедийные материалы Computer Science клуба (Санкт-Петербург). Курс «Сложность вычислений и основы криптографии», 2013, читает кандидат физико-математических наук, старший научный сотрудник лаборатории математической логики ПОМИ РАН, Д. М. Ицыксон (http://compsciclub.ru/courses/cryptography/2013-spring/?tab=classes).

4. Мультимедийные материалы Computer Science клуба (Санкт-Петербург). Курс «Теоретико-сложностные основы криптографии», 2016, читает кандидат физико-математических наук, старший научный сотрудник лаборатории математической логики ПОМИ РАН, Д. М. Ицыксон (http://compsciclub.ru/courses/cryptography-foundations/2016-spring/?tab=classes).

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения практических занятий, оснащенные средствами вычислительной техники, с установленным программным обеспечением Microsoft Visual Studio;
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

Автор(ы):

Доцент кафедры КБиММОИ, канд. физ.-мат. наук Д.М. Мурин

Приложение № 1 к рабочей программе дисциплины
«Сложностная криптография»

Фонд оценочных средств
для проведения текущего контроля успеваемости
и промежуточной аттестации студентов
по дисциплине

1. Типовые контрольные задания и иные материалы, используемые в процессе текущего контроля успеваемости

Задания для самостоятельной работы

Варианты заданий по теме № 1: «Односторонние функции».

Упражнение 1. Функция называется регулярной, если она принимает значения одинаковой длины на входах одинаковой длины. Докажите, что если существует односторонняя функция, то существует и регулярная односторонняя функция.

Упражнение 2. Функция называется сохраняющей длину, если она принимает значения, длина которых совпадает с длиной входов. Докажите, что если существует односторонняя функция, то существует и односторонняя функция, сохраняющая длину.

Упражнение 3. Постройте функцию, сохраняющую длину на всех длинах входов.

Упражнение 4. Изменится ли понятие «односторонняя функция», если в определении наделить нарушителя возможностью использовать детерминированную полиномиальную машину Тьюринга вместо вероятностной полиномиальной машины Тьюринга?

Упражнение 5. Изменится ли понятие «односторонняя функция», если предположить, что она (функция) является вычислимой за полиномиальное время на вероятностной машине Тьюринга, а не на детерминированной машине Тьюринга?

Упражнение 6. К каким последствиям может привести неравномерное распределение входных строк x на множестве $\{0, 1\}^n$?

Упражнение 7. Предполагая, что P не NP, постройте функцию f, для которой выполнены следующие три утверждения:

1. Функция f является полиномиально вычислимой.

2. Не существует полиномиального по времени алгоритма, который всегда обращает f (т. е. успешно обращает f на любом y из области значений f).

3. Функция f не является односторонней. Более того, существует полиномиальный по времени алгоритм, который обращает f с экспоненциально малой вероятностью ошибки (вероятность (как обычно) берется по всем возможным равномерно распределенным вариантам входа (т. е. $f(x)$) и исходам внутренних бросков честной монеты).

Упражнение 8. Пусть f является односторонней функцией и для некоторой функции $l : N \to N$ выполняются следующие условия:

1. для всех x: $|f(x)| = l(|x|)$;

2. $l(n) = l(m)$ только если $n = m$ (т. е. l является биективной функцией);

3. для всех n: $l(n) > n$.

Докажите, что для данной функции $f(x)$ можно сгенерировать $1^{|x|}$ за полиномиальное от $|x|$ время.

Упражнение 9 (Сложение легко обратимо). Сопоставим каким-то естественным образом двоичные слова положительными целым числам (например, двоичное слово $\sigma_{n-1} \ldots \sigma_0$ длины n сопоставим целому числу $2^n + \sigma_0 + \sigma_1 2 + \ldots + \sigma_{n-1} 2^{n-1}$:

1. Определим такую функцию $f_{add} : \{0, 1\}^* \to \{0, 1\}^*$, что $f_{add}(xy) = x+y$, где $|x| = |y|$.

Докажите, что f_{add} не является односторонней (даже в слабом смысле).

2. Переопределим функцию $f_{add} : \{0, 1\}^* \to \{0, 1\}^*$ таким образом, что $f_{add}(xy) = \mathrm{prime}(x) + \mathrm{prime}(y)$, где $|x| = |y|$ и $\mathrm{prime}(z)$ — наименьшее простое число, большее z. Докажите, что f_{add} не является односторонней.

В качестве разминки докажите, что $f_{XOR}(xy) = x \oplus y$, где $|x| = |y|$, не является односторонней.

Задания по теме № 2: «Семейство односторонних функций. Трудный бит».

Упражнение 1. Докажите, что односторонние функции существуют тогда и только тогда, когда существуют семейства односторонних функций.

Упражнение 2. Сгенерируем k случайных равномерно распределенных битовых строк длины n: $s_1, s_2, \ldots, s_k$. Для каждого $J \subset \{1, 2, \ldots, k\}, J \neq \varnothing$ определим строку $r_J = \oplus_{i \in J} s_i$. Покажите, что все r_J одинаково распределены и попарно независимы.

Упражнение 4. Изменится ли понятие «семейство односторонних функций», если в определении наделить нарушителя возможностью использовать детерминированную полиномиальную машину Тьюринга вместо вероятностной полиномиальной машины Тьюринга?

Упражнение 5. Изменится ли понятие «семейство односторонних функций», если предположить, что оно (семейство) является вычислимым за полиномиальное время на вероятностной машине Тьюрина, а не на детерминированной машине Тьюринга?

Упражнение 6. Доказать, что если существует односторонняя функция, то существует и неуниверсальная односторонняя функция.

Задания по теме № 3: «Генераторы псевдослучайных чисел».

1. Докажите, что отношение «быть вычислительно неразличимым» рефлексивно, симметрично и транзитивно.

2. Пусть α_n и β_n вычислительно неразличимы, $q(n)$ – полином, $U_{q(n)}$ - случайная величина, определенная и равномерно распределенная на битовых строках длины $q(n)$. Докажите, что $\alpha_n U_{q(n)}$ и $\beta_n U_{q(n)}$ вычислительно неразличимы.

3. Пусть α_n и β_n вычислительно неразличимы, f – полиномиально вычислимая функция. Докажите, что $f(\alpha_n)$ и $f(\beta_n)$ вычислительно неразличимы.

Задания по теме № 4: «Псевдослучайные функции».

1. Существует ли какой-нибудь конкретный тест, из которого следует случайность по всем остальным?

2. Постройте из псевдослучайного генератора $G: B^n \to B^N$ псевдослучайную функцию $F: n \times \log N \to \{0,1\}$.

Задания по теме № 5: «Привязка к биту».

1. Зафиксирует простое число p и первообразный корень $g \in Z_p^*$. Рассмотрим следующий протокол привязки к биту b:

Алиса выбирает случайное натуральное число $q \in \{2, \ldots, q-2\}$ и вычисляет $y = g^q \bmod p$.

Алиса посылает Бобу y.

Боб выбирает случайное натуральное число $r \in \{2, \ldots, q-2\}$ и вычисляет $C(b, r) = y^b g^r$.

Обладает ли данный протокол свойствами вычислительной связанности, безусловной связанности и безусловной секретности?

2. Могут ли одновременно достигаться и безусловная связанность и безусловная секретность?

Задания по теме № 6: «Доказательства с нулевым разглашением».

1. Доказать, что $PZK \subseteq CZK$.

2. Доказать, что $IP \subseteq PSPACE$.

3. Нулевое разглашение для квадратичных вычетов по составному модулю:

рассмотрим только те остатки x в классе вычетов по модулю $N = pq$, где p и q – простые, которые либо являются квадратичными вычетами по модулю N, либо не являются квадратичными вычетами ни по модулю p, ни по модулю q. Рассмотрим язык Li, который состоит только из тех остатков, которые являются квадратичными вычетами по модулю N. Предложите интерактивное доказательство с нулевым разглашением, которое доказывает принадлежность рассматриваемого остатка к языку Li.

Задания по теме № 7: «Шифрование с открытым ключом».

1. Доказать, что из существования надежной системы шифрования с открытым ключом следует существование семейства односторонних функций с секретом.

2. Предположим, что противник может использовать только детерминированные машины Тьюринга. Постройте криптосистему, полную в классе криптосистем с таким противником.

3. Будет ли существование семейства односторонних перестановок эквивалентно существованию одной односторонней перестановки?

4. Докажите, что если существует протокол с открытым ключом для сообщений из 1 бита, то существует протокол с открытым ключом для сообщений произвольной полиномиальной длины.

Задания по теме № 8: «Цифровые подписи».

1. Доказать, что существование семейств хеш-функций без коллизий влечет существование односторонних функций.

2. Докажите, что функция Рабина $f_m(x) = x^2 \bmod m$, где $m = pq$, p, q – простые числа представимые в виде $4k + 3$ при натуральном k, задает перестановку на множестве квадратичных вычетов по модулю m.

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

Список вопросов к экзамену:

1. «Честные» функции, односторонние в наихудших случаях функций, теорема о существовании односторонних в наихудших случаях функции при P ≠ NP. Сильные и слабые односторонние функции.
2. Эквивалентность существования сильной и слабой односторонних функций.
3. Семейство односторонних функций. Универсальная односторонняя функция. Теорема об универсальной функции Левина. Трудный бит (определение).
4. Теорема Голдрейха-Левина.
5. Генераторы псевдослучайных чисел. Вычислительная неразличимость. Теорема Голдрейха-Импальяццио-Луби-Хастада.
6. Теорема о $p(n)$-генераторе. Протоколы с секретным ключом.
7. Неразличимость с полиномиальным количеством образцов. Полиномиально моделируемые распределения. Теорема о неразличимости полиномиального числа образцов.
8. Ансамбли функций. Псевдослучайные ансамбли функций. Эффективно вычислимые ансамбли функций. Конструкция псевдослучайного ансамбля функций.
9. Теорема об эффективно вычислимом ансамбле псевдослучайных функций (описание алгоритма «D»).
10. Теорема об эффективно вычислимом ансамбле псевдослучайных функций (полагаем алгоритм «D» заданным).
11. Протоколы привязки к биту. Неинтерактивные протоколы. Теорема об условном существовании неинтерактивных протоколов привязки к биту.
12. Протоколы привязки к биту. Интерактивные протоколы. Теорема об условном существовании интерактивных протоколов привязки к биту.
13. Доказательства с нулевым разглашением. Интерактивные системы доказательства.

14. Доказательства с нулевым разглашением. Совершенно нулевое разглашение. Вычислительно нулевое разглашение.
15. Статистическая неразличимость. Односторонние перестановки. Теоремы о вычислительной неотличимости распределений случайных величин.
16. Семейства односторонних перестановок с секретом.
17. Шифрование с открытым ключом.
18. Цифровая подпись одного бита. Теорема об условном существовании протокола цифровой подписи одного бита.
19. Цифровая подпись фиксированного числа бит. Теорема об условном существовании протокола цифровой подписи фиксированного числа бит.
20. Цифровая подпись сообщений произвольной длины. Построение СТОК и СТОЗ.
21. Протокол подписи сообщений произвольной длины на основе односторонней функции.
22. Протокол подписи произвольного количества сообщений произвольной длины
23. Ансамбль распределений. Определения Левина и Импальяццо сложности в среднем, их эквивалентность.
24. Классы распределенных задач распознавания. Пример распределения, для которого сложность в худшем и в среднем случаях совпадают.

Правила выставления оценки на экзамене.

В экзаменационный билет включаются два теоретических вопроса. На подготовку к ответу дается не менее 1 академического часа.

По итогам экзамена выставляется одна из оценок: «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Оценка «Отлично» выставляется студенту, который демонстрирует глубокое и полное владение содержанием материала и понятийным аппаратом сложностной криптографии; умеет связывать теорию с практикой. Студент дает развернутые, полные и четкие ответы на вопросы экзаменационного билета и дополнительные вопросы, соблюдает логическую последовательность при изложении материала. Грамотно использует терминологию.

Оценка «Хорошо» выставляется студенту, ответ которого на экзамене в целом соответствуют указанным выше критериям, но отличается меньшей обстоятельностью, глубиной, обоснованностью и полнотой. В ответе имеют место отдельные неточности (несущественные ошибки), которые исправляются самим студентом после дополнительных и (или) уточняющих вопросов экзаменатора.

Оценка «Удовлетворительно» выставляется студенту, который дает недостаточно полные и последовательные ответы на вопросы экзаменационного билета и дополнительные вопросы, но при этом демонстрирует умение выделить существенные и несущественные признаки и установить причинно-следственные связи. Ответы излагаются с использованием терминологии сложностной криптографии, но при этом допускаются ошибки в определениях некоторых основных понятий, формулировках положений, которые студент затрудняется исправить самостоятельно. При аргументации ответа студент не обосновывает свои суждения. На часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Неудовлетворительно» выставляется студенту, который демонстрирует разрозненные, бессистемные знания; беспорядочно и неуверенно излагает материал; не умеет выделять главное и второстепенное, не умеет соединять теоретические положения с практикой; допускает грубые ошибки при определении сущности раскрываемых понятий, вследствие непонимания их существенных и несущественных признаков и связей; дает неполные ответы, логика и последовательность изложения которых имеют существенные и принципиальные нарушения, в ответах отсутствуют выводы. Дополнительные и уточняющие вопросы экзаменатора не приводят к коррекции ответов студента. На основную часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Неудовлетворительно» выставляется также студенту, который взял экзаменационный билет, но отказался дать на него ответ.

Приложение № 2 к рабочей программе дисциплины «Сложностная криптография»

Методические указания для студентов по освоению дисциплины

Учебным планом на изучение дисциплины «Сложностная криптография» отводится один семестр, по завершении которого в качестве итогового контроля предусмотрен экзамен. В процессе изучения дисциплины выполняются восемь домашних заданий.

При изучении учебного материала по дисциплине «Сложностная криптография» соблюдается баланс между лекционными и практическими занятиями. Это связано с тем, что с одной стороны в рамках дисциплины излагается большое количество нетривиального учебного материала, в том числе результаты научных исследований последнего десятилетия, а, с другой стороны, для полноценного освоения данного материала обучающемуся необходимо получить самостоятельный опыт по применению изучаемого в рамках дисциплины математического аппарата.

Основную роль для анализа и контроля качества усвоения материала играют домашние работы. В качестве заданий для самостоятельной работы дома обучающимся предлагаются математические задачи, которые должны позволить студенту переосмыслить изученные на лекциях понятия и методы, применить их для решения типовых задач из соответствующих разделов дисциплины. Решения задач должны быть подготовлены, оформлены в письменном виде и представлены в установленные сроки.

Для повышения качества усвоения теоретического материала, приобретенных практических навыков работы с изучаемым в рамках дисциплины математическим аппаратом проводятся консультации по разбору заданий для самостоятельной работы. Также на консультациях, возможно повторно, разъясняются вопросы, вызвавшие затруднения у обучающихся.

По итогам изучения дисциплины обучающиеся сдают экзамен. Экзамен принимается по экзаменационным билетам, каждый из которых включает в себя два теоретических вопроса. На самостоятельную подготовку к экзамену выделяется 3 дня, во время подготовки к экзамену предусмотрена групповая консультация.

Опыт преподавания дисциплины «Сложностная криптография» говорит о высокой сложности ее самостоятельного изучения для обучающегося в первую очередь ввиду достаточно узкого выбора учебной литературы на русском языке, а также ввиду необходимости обладания достаточно глубокими знаниями теории алгоритмов, теории вероятностей и математической статистики. Излагаемый на лекциях материал часто является нетривиальным и отражает результаты научных исследований последнего десятилетия. Поэтому посещение всех аудиторных занятий является обязательным.