ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА
(РОСАВИАЦИЯ)
ФГБОУ ВО «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ»
(ФГБОУ ВО СПбГУ ГА)

УТВЕРЖДАЮ
Первый
проректор-проректор
по учебной работе
_____ Н.Н. Сухих
«_16_» _апреля_____ 2019 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы криптографии

Направление подготовки
01.03.04 Прикладная математика

Направленность программы (профиль)
Математическое и программное обеспечение систем управления

Квалификация выпускника
бакалавр

Форма обучения
очная

Санкт-Петербург
2019

1 Цели освоения дисциплины

Целями освоения дисциплины «Основы криптографии» являются формирование у обучающихся комплекса теоретических знаний математических подходов к решению задач компьютерной безопасности и, прежде всего, к построению криптографических алгоритмов, а также приобретение ими умений и практических навыков использования математического аппарата для вывода свойств разрабатываемых методов, умению самостоятельно повышать свои знания в области криптографии и защиты информации.

Задачами освоения дисциплины «Основы криптографии» являются:

– формирование у обучающихся знаний об основных результатах в области криптографических исследований;

– приобретение обучающимися умений анализировать методы криптографии при решении задач защиты информации;

– овладение обучающимися навыками решения основных криптографических задач.

Дисциплина обеспечивает подготовку выпускника к научно-исследовательскому типу профессиональной деятельности.

2 Место дисциплины в структуре ОПОП ВО

Дисциплина «Основы криптографии» представляет собой дисциплину, относящуюся к блоку Факультативы.

Дисциплина «Основы криптографии» базируется на результатах обучения, полученных при изучении дисциплин: «Алгоритмы и структуры данных», «Теория сложных вычислений и алгоритмов».

Дисциплина «Основы криптографии» изучается в 7 семестре.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс освоения дисциплины «Основы криптографии» направлен на формирование следующих компетенций:

Перечень и код компетенций	Перечень планируемых результатов обучения по дисциплине
Способен разрабатывать алгоритмы и реализовывать их на основе современных парадигм, технологий и языков программирования	Знать: – основные информационные источники, содержащие термины и понятия, относящиеся к криптографии; – математические основы современной криптографии; показатели и проблемы стойкости криптосистем; Уметь: – самостоятельно анализировать модели обеспечения информационной безопасности; – осуществлять программную реализацию

Перечень и код компетенций	Перечень планируемых результатов обучения по дисциплине
(ПК-2)	криптографических алгоритмов; Владеть: – навыками использования криптографических методов; – методами оценки эффективности криптографических систем.

4 Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 академических часа.

Наименование	Всего часов	Семестр
		7
Общая трудоемкость дисциплины	108	108
Контактная работа:	28,3	28,3
лекции	14	14
практические занятия	14	14
семинары	–	–
лабораторные работы	–	–
курсовой проект (работа)	–	–
Самостоятельная работа студента	71	71
Промежуточная аттестация	9	9
контактная работа	0,3	0,3
самостоятельная работа по подготовке к зачету	8,7	8,7

5 Содержание дисциплины

5.1 Соотнесения тем (разделов) дисциплины и формируемых компетенций

Темы (разделы) дисциплины	Количество часов	Компетенции	Образовательные технологии	Оценочные средства
		ПК-2		
Тема 1. Обеспечение информационной безопасности деятельности общества. Модели обеспечения информационной	30	+	ВК, ПЗ, СРС	Д

Темы (разделы) дисциплины	Количество часов	Компетенции	Образовательные технологии	Оценочные средства
		ПК-2		
безопасности				
Тема 2. Симметричные и ассиметричные криптографические системы	31	+	ПЗ, СРС	П
Тема 3. Электронные цифровые подписи.	38	+	ПЗ, СРС	П
Всего по дисциплине	99			
Промежуточная аттестация	9			
Итого по дисциплине	108			

ПЗ – практическое занятие, СРС – самостоятельная работа студента, ВК – входной контроль, П – проект, Д – доклад.

5.2 Темы (разделы) дисциплины и виды занятий

Наименование темы (раздела) дисциплины	Л	ПЗ	С	ЛР	СРС	КР	Всего часов
Тема 1. Обеспечение информационной безопасности деятельности общества. Модели обеспечения информационной безопасности	4	4	-	-	22	-	30
Тема 2. Симметричные и ассиметричные криптографические системы	4	4	-	-	23	-	31
Тема 3. Электронные цифровые подписи и криптографические ключи.	6	6	-	-	26	-	38
Всего по дисциплине	14	14	-	-	71	-	99
Промежуточная аттестация							9
Итого по дисциплине							108

Л – лекция, ПЗ – практическое занятие, СРС – самостоятельная работа студента, С – семинар, ЛР – лабораторная работа, КР – курсовая работа (проект).

5.3 Содержание дисциплины

Тема 1. Обеспечение информационной безопасности деятельности общества. Модели обеспечения информационной безопасности

Информационная безопасность деятельности общества и ее основные положения. Организационные, физико-технические, информационные и

программно-математические угрозы. Эволюция подходов к обеспечению информационной безопасности. Стратегии, модели и системы предотвращения несанкционированного доступа в информационные системы. Критерии и классы оценки защищенности объектов и деятельности.

Тема 2. Симметричные и ассиметричные криптографические системы

Основные классы симметричных криптосистем. Блочные шифры. Алгоритмы блочного шифрования. Режимы применения блочных шифров. Потоковые шифры. Ассиметричные шифры. Односторонние функции и функции ловушки. Ассиметричные системы шифрования

Тема 3. Электронные цифровые подписи и криптографические ключи

Постановка задачи. Алгоритмы электронной цифровой подписи. Функции хэширования. Обычная система управления ключами. Управление ключами, основанное на системах с открытым ключом. Протокол обмена секретным ключом. Использование сертификатов. Протоколы аутентификации. Анонимное распределение ключей.

5.4 Практические занятия (семинары)

Номер темы дисциплины	Тематика практических занятий (семинаров)	Трудоемкость (часы)
1	Практическое занятие №1. Классификация видов угроз информационной безопасности. Эволюция подходов к обеспечению информационной безопасности	2
	Практическое занятие №2. Комплексное информационное обеспечение безопасности государства.	2
2	Практическое занятие №3. Анализ алгоритмов DES, алгоритм Rijndael, RC6.	2
	Практическое занятие №4. Программная реализация алгоритмов шифрования.	2
3	Практическое занятие №5. Стандарты электронной цифровой подписи. Анализ алгоритмов цифровой подписи, основанных на ассиметричных криптосистемах.	2
	Практическое занятие №6. Программная реализация алгоритма хэширования.	2
	Практическое занятие № 7-8. Управление ключами, основанное на системах с открытым ключом. Использование сертификатов.	2
Итого по дисциплине:		14

5.5 Лабораторный практикум

Лабораторный практикум учебным планом не предусмотрен.

5.6 Самостоятельная работа

Номер темы дисциплины	Виды самостоятельной работы	Трудо-емкость (часы)
1	1. Поиск, анализ информации и проработка учебного материала [1, 2, 3]. 2. Подготовка к докладу.	22
2	1. Поиск, анализ информации и проработка учебного материала [1,4,5-14]. 2. Подготовка к проекту.	23
3	1. Поиск, анализ информации и проработка учебного материала [1,4,5-14]. 2. Подготовка к проекту.	26
Итого по дисциплине		71

5.7 Курсовые работы (проекты)

Курсовые работы (проекты) учебным планом не предусмотрены.

6 Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Фомичёв, В. М. **Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты** : учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под ред. В. М. Фомичёва. — М. : Издательство Юрайт, 2017. — 209 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-01740-3. — Режим доступа : www.biblio-online.ru/book/A01C7E90-A5B7-4B50-B348-31CB49CA5B3D .

2. Нестеров, С.А. **Основы информационной безопасности** [Электронный ресурс] : учебное пособие / С.А. Нестеров. — Электрон. дан. — Санкт-Петербург : Лань, 2018. — 324 с. — Режим доступа: https://e.lanbook.com/book/103908 . — Загл. с экрана.

3. Фомичёв, В. М. **Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты: учебник для академического бакалавриата** / В. М. Фомичёв, Д. А. Мельников; под ред. В. М. Фомичёва. — М.: Издательство Юрайт, 2018. — 245 с. — (Серия: Бакалавр. Академический курс). — ISBN 978-5-9916-7090-6. — Режим доступа : www.biblio-online.ru/book/AF99BBDE-AF3A-43A9-A90F-B99806553C25

б) дополнительная литература:

4. Васильева, И. Н. **Криптографические методы защиты информации** : учебник и практикум для академического бакалавриата / И. Н. Васильева. — М. : Издательство Юрайт, 2017. — 349 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-02883-6. — Режим доступа : www.biblio-online.ru/book/38C7E67F-676F-4A9E-8E92-FD548EA095BA .

5. **Введение в теоретико-числовые методы криптографии** [Электронный ресурс] : учебное пособие / М.М. Глухов [и др.]. — Электрон. дан. — Санкт-Петербург: Лань, 2011. — 400 с. — Режим доступа: https://e.lanbook.com/book/68466 . — Загл. с экрана .

в) перечень ресурсов информационно-телекоммуникационной сети «Интернет»:

6. **Математическая криптография** [Электронный ресурс]. – Режим доступа: http://cryptography.ru/ . – Загл. с экрана. (дата обращения: 17.01.2018).

7. **Интернет-проект «Задачи»** [Электронный ресурс]. – Режим доступа: https://stepik.org/course/217/syllabus .– Загл. с экрана. (дата обращения: 17.01.2018).

8. **Параллель: Базовая электронная энциклопедия по параллельным вычислениям**. [Электронный ресурс]. – Режим доступа: http://www.problems.ru/ .– Загл. с экрана. (дата обращения: 27.03.2019).

г) программное обеспечение (лицензионное), базы данных, информационно-справочные и поисковые системы:

9 **Единое окно доступа к образовательным ресурсам** [Электронный ресурс]. – Режим доступа: http://window.edu.ru, свободный (дата обращения: 17.01.2018).

10 **Электронная библиотека научных публикаций «eLIBRARY.RU»** [Электронный ресурс] — Режим доступа: http://elibrary.ru/, свободный_ (дата обращения: 27.03.2019).

11 **Электронно-библиотечная система издательства «Лань»** [Электронный ресурс] — Режим доступа: http://e.lanbook.com/, свободный (дата обращения: 27.03.2019).

12 **Cygwin** [Электронный ресурс] — Режим доступа: https://www.cygwin.com/ - свободный (дата обращения: 27.03.2019).

13 **Сайт библиотеки GNU MP** [Электронный ресурс] — Режим доступа: http://gmplib.org – свободный (дата обращения: 27.03.2019).

14 **Сайт библиотеки GNU Crypto** [Электронный ресурс] — Режим доступа: http://www.gnu.org/s/gnu-crypto - свободный (дата обращения: 27.03.2019).

7 Материально-техническое обеспечение дисциплины

Компьютерные классы кафедры № 8 с доступом в Интернет, переносной проектор.

Информационно-справочные и материальные ресурсы библиотеки СПбГУ ГА.

Лицензионное программное обеспечение: Microsoft Office, Cygwin.

8 Образовательные и информационные технологии

Дисциплина «Основы криптографии» предполагает использование следующих образовательных технологий: входной контроль, практические занятия и самостоятельная работа студента.

Входной контроль проводится преподавателем в начале изучения дисциплины с целью коррекции процесса усвоения студентами дидактических единиц. Он осуществляется по вопросам из дисциплин, на которых базируется дисциплина «Основы криптографии» (п. 2).

Практическое занятие по дисциплине «Основы криптографии» содействует выработке у обучающихся умений и навыков применения знаний, полученных в ходе самостоятельной работы. Практические занятия как образовательная технология помогает студентам систематизировать, закрепить и углубить знания.

Самостоятельная работа студента проявляется в систематизации, планировании, контроле и регулировании его учебно-профессиональной деятельности, а также собственные познавательно-мыслительные действия без непосредственной помощь и руководства со стороны преподавателя. Основной целью самостоятельной работы студента является формирование навыка самостоятельного приобретения им знаний по некоторым несложным вопросам теоретического курса, закрепление и углубление полученных знаний, умений и навыков во время практических занятий. Самостоятельная работа подразумевает выполнение студентом поиска, анализа информации, проработку на этой основе учебного материала, подготовку к докладу, а также подготовку проекта.

В рамках изучения дисциплины «Основы криптографии» предполагается использовать в качестве информационных технологий среду MS Office, Cygwin.

9 Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины

Фонд оценочных средств дисциплины «Основы криптографии» представляет собой комплекс методических и контрольных измерительных материалов, предназначенных для определения качества результатов обучения и уровня сформированности компетенций обучающихся в ходе освоения данной дисциплины. В свою очередь, задачами использования фонда оценочных средств являются осуществление как текущего контроля успеваемости студентов, так и промежуточной аттестации в форме зачета.

Фонд оценочных средств дисциплины «Основы криптографии» для текущего контроля включает: проект и доклад.

Доклад представляет собой публичное выступление по представлению полученных результатов анализа определенной учебно-исследовательской темы. Типовые темы докладов представлены в п. 9.4.

Проект предназначен для проверки умений и навыков самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве. Проект является конечным программным продуктом.

Промежуточная аттестация по итогам освоения дисциплины проводится в виде зачета в 6 семестре. Этот вид промежуточной аттестации позволяет оценить уровень освоения студентом компетенций за весь период изучения дисциплины. Зачет предполагает устные ответы на 2 теоретических вопроса из перечня вопросов, вынесенных на промежуточную аттестацию, а также решение задачи.

9.1. Балльно-рейтинговая оценка текущего контроля успеваемости и знаний студентов

Тема/вид учебных занятий (оценочных заданий), позволяющих студенту продемонстрировать достигнутый уровень сформированности компетенций	Количество баллов		Срок контроля (порядковый номер недели с начала семестра)	Примечание
	минимальное значение	максимальное значение		
Контактная работа				
Аудиторные занятия				
Лекция №1 (Тема 1)	3	5	1	
Практическое занятие №1 (Тема 1)	3	5	2	
Лекция №2 (Тема 1)	3,5	5	3	
Практическое занятие №2 (Тема 1)	3	5	4	
Лекция №3 (Тема 2)	3,5	5	5	
Практическое занятие №3 (Тема 2)	3	5	6	
Лекция №4 (Тема 2)	3,5	5	7	
Практическое занятие №4 (Тема 2)	3	5	8	
Лекция №5 (Тема 3)	3,5	5	9	
Практическое занятие №5 (Тема 3)	3	5	10	
Лекция №6 (Тема 3)	3,5	5	11	
Практическое занятие №6 (Тема 3)	3	5	12	
Лекция №7 (Тема 3)	3,5	5	13	
Практическое занятие №7 (Тема 3)	3	5	14	
Итого по обязательным видам занятий	**45**	**70**		
Зачет	**15**	**30**		
Итого по дисциплине	**60**	**100**		
Премиальные виды деятельности (для учета при определении рейтинга)				
Научные публикации по темам дисциплины		10		
Участие в конференциях по темам дисциплины		10		
Итого дополнительно премиальных баллов		**20**		
Всего по дисциплине для рейтинга		**120**		

Перевод баллов балльно-рейтинговой системы в оценку для зачета	
Количество баллов по БРС	**Оценка**
60 и более	«зачтено»
менее 60	«не зачтено»

9.2 Методические рекомендации по проведению процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Посещение обучающимся лекционного занятия с ведением конспекта оценивается от 3 до 3,5 баллов. Ответы на вопросы, возникающие в ходе лекции и активное участие в их обсуждении – от 1,5 до 2 баллов.

Посещение обучающимся практического занятия с ведением конспекта оценивается в 3 балла. Выступление с докладом – до 1 балла. Проект – до 1 балла.

9.3 Темы курсовых работ (проектов) по дисциплине

Написание курсовых работ (проектов) учебным планом не предусмотрено.

9.4 Контрольные задания для проведения входного контроля остаточных знаний по обеспечивающим дисциплинам

1. Формальное определение алгоритма.
2. Пример вычислительной проблемы.
3. Формальное описание алгоритма. Отличия от кода языка высокого уровня.
4. Роль асимптотической нотации в определении производительности алгоритмов и структур данных.
5. Амортизационный анализ – назначение и примеры использования.

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

<table>
<tr><th>Критерий</th><th>Этапы формирования</th><th>Показатель</th></tr>
<tr><td colspan="3">Способен разрабатывать алгоритмы и реализовывать их на основе современных парадигм, технологий и языков программирования (ПК-2)</td></tr>
<tr><td rowspan="2">Знать:
– основные информационные источники, содержащие термины и понятия, относящиеся к криптографии;</td><td>1 этап формирования</td><td>– самостоятельно находит информационные источники, относящиеся к криптографическому анализу;</td></tr>
<tr><td>2 этап формирования</td><td>– выделяет из имеющейся избыточной информации необходимую для решения поставленной задачи;</td></tr>
</table>

Критерий	Этапы формирования	Показатель
– математические основы современной криптографии; показатели и проблемы стойкости криптосистем	1 этап формирования	- называет основные классы криптосистем, простейшие шифры и их свойства;
	2 этап формирования	- строит математические модели шифров, классифицирует показатели стойкости криптосистем;
Уметь: – самостоятельно анализировать модели обеспечения информационной безопасности.	1 этап формирования	- воспроизводит модели обеспечения информационной безопасности
	2 этап формирования	- анализирует стратегии обеспечения информационной безопасности, оценивает защищенность процессов переработки информации;
– осуществлять программную реализацию криптографических алгоритмов	1 этап формирования	- составляет криптографические алгоритмы с использованием псевдокода и (или) блок-схем;
	2 этап формирования	- определяет криптографический алгоритм и составляет его с использованием заданного языка программирования;
Владеть: – навыками использования криптографических методов	1 этап формирования	- перечисляет основные криптографические задачи и методы их решения;
	2 этап формирования	– объясняет и применяет методы решения основных криптографических задач;
Владеть: - методами оценки эффективности криптографических систем	1 этап формирования	- перечисляет типы основных способов криптоанализа шифров, способы построения хеш-функций и основные требования к ним, основные типы электронной подписи и криптографических протоколов;
	2 этап формирования	– - анализирует эффективность хеш-функций, классифицирует основные типы электронной подписи, оценивает их эффективность.

Характеристики шкалы оценивания приведены ниже.

1. Максимальное количество баллов за зачет – 30. Минимальное (зачетное) количество баллов – 15 баллов (что соответствует «зачтено»).
2. При наборе менее 15 баллов – зачет не сдан по причине недостаточного уровня знаний.
3. «Зачтено» выставляется как сумма набранных баллов за ответы на вопросы билета и за решение задачи.
4. Ответы на вопросы оцениваются следующим образом:

– *1 балл*: отсутствие продемонстрированных знаний и компетенций в рамках образовательного стандарта (нет ответа на вопрос) или отказ от ответа;

– *2 балла*: нет удовлетворительного ответа на вопрос, демонстрация фрагментарных знаний в рамках образовательного стандарта, незнание лекционного материала;

– 3 *балла*: нет удовлетворительного ответа на вопрос, много наводящих вопросов, отсутствие ответов по основным положениям вопроса, незнание лекционного материала;

– *4 балла*: ответ удовлетворительный, оценивается как минимально необходимые знания по вопросу, при этом студентом продемонстрировано хотя бы минимальное знание всех разделов вопроса в пределах лекционного материала. При этом студентом демонстрируется достаточный объем знаний в рамках образовательного стандарта;

– *5 баллов*: ответ удовлетворительный, достаточные знания в объеме учебной программы, ориентированные на воспроизведение; использование научной (технической) терминологии, стилистически грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;

– *6 баллов*: ответ удовлетворительный, студент достаточно ориентируется в основных аспектах вопроса, демонстрирует полные и систематизированные знания в объеме учебной программы;

– 7 *баллов*: ответ хороший (достаточное знание материала), но требовались наводящие вопросы, студент демонстрирует систематизированные, глубокие и полные знания по всем разделам учебной программы;

– *8 баллов*: ответ хороший, ответом достаточно охвачены все разделы вопроса, единичные наводящие вопросы; студент демонстрирует способность самостоятельно решать сложные проблемы в рамках учебной программы;

– *9 баллов*: систематизированные, глубокие и полные знания по всем разделам учебной программы; студент демонстрирует способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации в рамках учебной программы;

– *10 баллов*: ответ на вопрос полный, не было необходимости в дополнительных (наводящих вопросах); студент демонстрирует систематизированные, глубокие и полные знания по всем разделам учебной программы, а также по основным вопросам, выходящим за ее пределы.

5. Решение задачи оценивается следующим образом:

– *10 баллов*: задание выполнено на 91-100 %, решение и ответ аккуратно оформлены, выводы обоснованы, дана правильная и полная интерпретация выводов, студент аргументированно обосновывает свою точку зрения, уверенно и правильно отвечает на вопросы предподавателя;

– *9 баллов*: задание выполнено на 86-90 %, решение и ответ аккуратно оформлены, выводы обоснованы, дана правильная и полная интерпретация выводов, студент аргументированно обосновывает свою точку зрения, правильно отвечает на вопросы предподавателя;

– *8 баллов*: задание выполнено на 81-85 %, ход решения правильный, незначительные погрешности в оформлении; правильная, но не полная интерпретация выводов, студент дает верные, но не полные ответы на вопросы преподавателя, испытывает некоторые затруднения в интерпретации полученных выводов;

– *7 баллов*: задание выполнено на 74-80 %, ход решения правильный, значительные погрешности в оформлении; правильная, но не полная интерпретация выводов, студент дает правильные, но не полные ответы на вопросы преподавателя, испытывает определенные затруднения в интерпретации полученных выводов;

– *6 баллов*: задание выполнено 66-75 %, подход к решению правильный, есть ошибки, оформление с незначительными погрешностями, неполная интерпретация выводов, не все ответы на вопросы преподавателя правильные, не способен интерпретировать полученные выводы;

– *5 баллов*: задание выполнено на 60-65 %, подход к решению правильный, есть ошибки, значительные погрешности при оформлении, неполная интерпретация выводов, не все ответы на вопросы преподавателя правильные, не способен интерпретировать полученные выводы;

– *4 балла*: задание выполнено на 55-59 %, подход к решению правильный, есть ошибки, значительные погрешности при оформлении, неполная интерпретация выводов, не все ответы на вопросы преподавателя правильные, не способен интерпретировать полученные выводы;

– *3 балла*: задание выполнено на 41-54 %, решение содержит грубые ошибки, неаккуратное оформление работы, неправильная интерпретация выводов, студент дает неправильные ответы на вопросы преподавателя;

– *2 балла*: задание выполнено на 20-40 %, решение содержит грубые ошибки, неаккуратное оформление работы, выводы отсутствуют; не может прокомментировать ход решения задачи, дает неправильные ответы на вопросы преподавателя;

– *1 балл:* задание выполнено менее, чем на 20 %, решение содержит грубые ошибки, студент не может прокомментировать ход решения задачи, не способен сформулировать выводы по работе.

9.6 Типовые контрольные задания для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины

Типовое задание для проекта.

Выполнить программную реализацию современного алгоритма блочного шифрования DES, используя язык программирования C++.

Типовые темы докладов:

6. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
7. Информация, основные свойства и характеристики безопасности ее применения.
8. Комплексное обеспечение информационной безопасности государства.
9. Области и объекты по обеспечению информационной безопасности и защите информационной деятельности.
10. Технологии обеспечения безопасности обработки информации.
11. Обеспечение информационной безопасности в нормальных и чрезвычайных ситуациях.

Перечень типовых вопросов к зачету для проведения промежуточной аттестации по дисциплине

1. Определение информационной безопасности.
2. Что такое доступность информации?
3. Какие возможные степени секретности Вы знаете?
4. Перечислите основные типы угроз информационной безопасности. Приведите примеры к каждому типу.
5. Какие основные эволюционные подходы к обеспечению информационной безопасности деятельности общества Вы знаете?
6. Сформулируйте основные проблемы информационной безопасности.
7. Каковы основные группы моделей безопасности?
8. Какие модели разграничения доступа Вы знаете?
9. Какие существуют критерии оценки защищенности объектов?
10. Алгоритм блочного шифрования DES и его модификации.
11. Алгоритм блочного шифрования AES. Алгоритм Rijndael.
12. Алгоритм блочного шифрования RC6.
13. Алгоритм блочного шифрования Safer.
14. Потоковое шифрование. Метод RC4.
15. Потоковое шифрование. Метод SEAL.
16. Потоковое шифрование. Метод WAKE.
17. Ассиметричная криптосистема шифрования Эль-Гамаля.
18. Криптосистема, основанная на проблеме Диффи-Хеллмана.
19. Алгоритмы цифровой электронной подписи.
20. Стандарты цифровой электронной подписи.

21. Функции хэширования. Достоинства и недостатки различных видов хэширования.

Типовая задача для промежуточной аттестации:

Описать (привести блок-схему или псевдокод) алгоритм симметричного шифрования. Режим выполнения алгоритма – простая замена.

10 Методические рекомендации для обучающихся по освоению дисциплины

Методика преподавания дисциплины «Основы криптографии» характеризуется совокупностью методов, приемов и средств обучения, обеспечивающих реализацию содержания и учебно-воспитательных целей дисциплины, которая может быть представлена как некоторая методическая система, включающая методы, приемы и средства обучения. Такой подход позволяет более качественно подойти к вопросу освоения дисциплины обучающимися.

Основными видами учебных занятий по дисциплине являются практические занятия. Объем и виды учебных занятий определены представленной рабочей программой дисциплины.

Практические занятия по дисциплине имеют целью:

- углубление, расширение и конкретизацию знаний, до уровня, на котором возможно их практическое использование;
- отработку навыков и умений в пользовании соответствующем математическим аппаратом.

Основу практических занятий составляет работа каждого обучаемого индивидуальная и (или) коллективная, по приобретению умений и навыков использования закономерностей, принципов, методов, форм и средств, составляющих содержание дисциплины в профессиональной деятельности и в подготовке к изучению дисциплин, формирующих компетенции выпускника.

По результатам контроля знаний и умений преподаватель должен провести анализ хода и итогов практических занятий, отметить успехи студентов в решении учебной задачи, а также недостатки и ошибки, разобрать их причины и дать методические указания к их устранению. Таким образом, практические занятия являются важной формой обучения, в ходе которых знания студентов превращаются в профессиональные необходимые умения, навыки.

Зачет являются заключительными оценочным средством, по итогам которого выявляется общий уровень овладения обучающимися предусмотренных компетенций по тематическим вопросам всего курса.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 01.03.04 «Прикладная математика».

Программа рассмотрена и утверждена на заседании кафедры №8 Прикладной математики и информатики

«9» апреля 2019 года, протокол № 9.

Разработчики:

к.т.н., доцент Далингер Я.М.
(ученая степень, ученое звание, фамилия и инициалы разработчиков)

к.т.н. Земсков Ю.В.
(ученая степень, ученое звание, фамилия и инициалы разработчиков)

Заведующий кафедрой № 8 Прикладной математики и информатики

к.т.н., доцент Далингер Я.М.
(ученая степень, ученое звание, фамилия и инициалы заведующего кафедрой)

Программа согласована:

Руководитель ОПОП

к.т.н., доцент Далингер Я.М.
(ученая степень, ученое звание, фамилия и инициалы руководителя ОПОП)

Программа рассмотрена и одобрена на заседании Учебно-методического совета Университета «16» апреля 2019 года, протокол № 6.