МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

Кафедра №51

«УТВЕРЖДАЮ»
Руководитель направления
зав. каф., к.т.н., доц.
_____А.А. Овчинников
«15» мая 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Криптографические методы защиты информации»
(Название дисциплины)

Код направления	10.03.01
Наименование направления/ специальности	Информационная безопасность
Наименование направленности	Комплексная защита объектов информатизации
Форма обучения	очная

Санкт-Петербург 2019 г.

Лист согласования рабочей программы дисциплины

Программу составил

доц., к.т.н., доц. _____15.05.2019 А.А. Овчинников

подпись, дата

Программа одобрена на заседании кафедры № 51

«15» мая 2019 г., протокол №10

Заведующий кафедрой № 51

доц., к.т.н., доц. _____15.05.2019 А.А. Овчинников

подпись, дата

Ответственный за ОП 10.03.01(03)

доц., к.т.н., доц. _____15.05.2019 А.А. Овчинников

подпись, дата

Заместитель директора института (факультета) № 5 по методической работе

доц., к.т.н., доц. 15.05.2019 О.И. Красильникова

должность, уч. степень, звание подпись, дата инициалы, фамилия

Аннотация

Дисциплина «Криптографические методы защиты информации» входит в базовую часть образовательной программы подготовки обучающихся по направлению 10.03.01 «Информационная безопасность» направленность «Комплексная защита объектов информатизации». Дисциплина реализуется кафедрой №51.

Дисциплина нацелена на формирование у выпускника

общепрофессиональных компетенций:

ОПК-2 «способность применять соответствующий математический аппарат для решения профессиональных задач»;

профессиональных компетенций:

ПК-1 «способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации»,

ПК-12 «способность принимать участие в проведении экспериментальных исследований системы защиты информации».

Содержание дисциплины охватывает круг вопросов, связанных с связанных с защитой компьютерной информации, существующих методов и информационных технологий этой защиты и оценкой их стойкости в информационных системах.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа студента.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме экзамена.

Общая трудоемкость освоения дисциплины составляет 6 зачетных единиц, 216 часов.

Язык обучения по дисциплине «русский».

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Цель курса - научить студентов понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности.

В курс включены основные методы криптографии, применяемые в защите информации. Анализ криптографических алгоритмов органически связан с синтезом криптоалгоритмов и криптопротоколов. В результате изучения курса студенты должны получить представление об основном криптографическом инструментарии, необходимом для использования защищенных информационных систем.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-2 «способность применять соответствующий математический аппарат для решения профессиональных задач»:

знать – методику применения теории NP-полных задач для обоснования стойкости криптосистем; основные методы решения трудных теоретико-числовых проблем;

уметь – оценивать стойкость теоретико-числовых криптосистем с открытым ключом;

владеть навыками – построения и анализа вычислительно трудных теоретико- числовых функций и применения этих функций в задачах защиты информации;

иметь опыт деятельности – решения задач защиты информации;

ПК-1 «способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации»:

знать – методы построения информационных средств и технологий защиты информации

уметь – самостоятельно изучать и строить математические модели криптоалгоритмов

владеть навыками – употребления отечественной терминологии в области криптографии для выражения количественных и качественных требований по защите информации;

иметь опыт деятельности – по использованию математического аппарата в проведении исследований;

ПК-12 «способность принимать участие в проведении экспериментальных исследований системы защиты информации»:

знать – методическое обеспечение проведения экспериментальных исследований системы защиты информации;

уметь – разработать криптографическую модель системы защиты информации;

владеть навыками – построения моделирующего алгоритма системы защиты информации;

иметь опыт деятельности – участия в проведении экспериментальных исследований системы защиты информации.

2. Место дисциплины в структуре ОП

Дисциплина базируется на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

- Алгоритмические проблемы криптографии
- Дискретная математика
- Математика. Теория вероятностей и математическая статистика

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и используются при изучении других дисциплин:

– Техническая защита информации;
– УИРС.

3. Объем дисциплины в ЗЕ/академ. час

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 1

Таблица 1 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам	
		№5	№6
1	2	3	4
Общая трудоемкость дисциплины, ЗЕ/(час)	6/ 216	3/ 108	3/ 108
Аудиторные занятия, всего час., ***В том числе***	85	51	34
лекции (Л), (час)	51	34	17
Практические/семинарские занятия (ПЗ), (час)			
лабораторные работы (ЛР), (час)	34	17	17
курсовой проект (работа) (КП, КР), (час)			
Экзамен, (час)	36		36
Самостоятельная работа, всего (час)	95	57	38
Вид промежуточного контроля: зачет, дифф. зачет, экзамен **(Зачет, Дифф. зач, Экз.)**	Зачет, Экз.	Зачет	Экз.

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий

Разделы и темы дисциплины и их трудоемкость приведены в таблице 2.

Таблица 2. – Разделы, темы дисциплины и их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 5					
Раздел 1. Основные понятия криптографии	10				15
Раздел 2. Симметричные шифры	24		17		35
Текущий контроль					7
Итого в семестре:	34		17		57
Семестр 6					
Раздел 3. Криптография с открытым ключом	11		11		20
Раздел 4. Криптографические протоколы	6		6		10

Текущий контроль					8
Итого в семестре:	17		17		38
Итого:	51	0	34	0	95

4.2. Содержание разделов и тем лекционных занятий

Содержание разделов и тем лекционных занятий приведено в таблице 3.

Таблица 3 - Содержание разделов и тем лекционных занятий

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	Раздел 1. Основные понятия криптографии. Тема 1.1 – Основные определения Определение целей и принципов защиты информации; установление, факторов, влияющих на защиту информации; основные опасности и угрозы в области информационной безопасности. Классификации видов, методов и средств защиты информации. Организационная защита информации. Инженерно- техническая защита информации. Криптографическая защита информации. Представление информации в цифровом виде. Тема 1.2 – Задачи информационной безопасности Задача обеспечения конфиденциальности. Определение шифра. Задача обеспечения аутентификации, понятия об электронной цифровой подписи (ЭЦП). Основные задачи в области управления ключами. Криптопротоколы: обеспечение идентификации, разделение секрета, выработка ключа, цифровые деньги.
2	Раздел 2. Симметричные шифры Тема 2.1. Исторические шифры Подстановочные шифры и перестановочные шифры. Шифр Цезаря, аффинный шифр, шифр моноалфавитной замены. Шифр Виженера. Цилиндр Джефферсона. Полиалфавитные шифры. Роторные машины. Тема 2.2. Блоковые шифры Понятие стойкости, предположения об исходных условиях криптоанализа, совершенная стойкость. Одноразовый блокнот. Шифр Вернама. Принципы построения блоковых шифров. Свойства смешивания и рассеивания. Составные шифры, итеративные шифры. SP-сети, сети Файстеля. Современные системы шифрования: алгоритмы DES, ГОСТ 28147-89, AES. Режимы блокового шифрования: ECB, CBC, CFB, OFB. Режим счетчика. Многократное шифрование. Тема 2.3. Потоковые шифры Требования к поточным шифрам. Методы построения больших периодов в поточных шифрах. Регистры сдвига с линейной обратной связью (РСЛОС). m-последовательности. Алгоритм Берлекэмпа-Месси. Построение потоковых шифров на основе РСЛОС. Нелинейное комбинирование РСЛОС: генератор Геффе, шифры с контролем тактов. Применение поточного шифрования.
3	Раздел 3. Криптография с открытым ключом Тема 3.1 - Математические основы систем с открытым ключом Модульная арифметика. Алгоритм Евклида и его сложность. Расширенный алгоритм Евклида. Основные теоремы о вычетах. Функция Эйлера. Теоремы Эйлера, Ферма. Факторизация.

	Логарифмирование в конечных полях. Оценки сложности “трудных” проблем, на которых строятся системы с открытым ключом. Быстрое возведение в степень. Тема 3.2 - Основные алгоритмы с открытым ключом Система Меркли-Хеллмана. Схема RSA. Атаки на RSA. Схема шифрования Эль-Гамаля. Система Мак-Элиса. Криптографические хэш-функции. Понятие о цифровой подписи. Подпись RSA. Подпись Эль-Гамаля. Подпись DSA. ЭЦП ГОСТ Р 34.10-94 и ГОСТ Р 34.10-01.
4	Раздел 4. Криптографические протоколы Тема 4.1 - Основные протоколы с открытым ключом Выработка ключа. Протокол Диффи-Хелмана. Гибридные системы шифрования: цифровой конверт. Доказательство с нулевым разглашением. Схема идентификации Фиата-Шамира. Схема идентификации Гиллу-Квискуотера. Инфраструктура открытых ключей. Сертификаты открытых ключей. Тема 4.2. – Специальные протоколы Слепая подпись. Протоколы разделения секрета и вручения бит. Протоколы цифровых денег и электронного голосования. Защищенные распределенные вычисления.

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 4.

Таблица 4 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	№ раздела дисципли-лины
Учебным планом не предусмотрено				

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	№ раздела дисциплины
Семестр 5			
1	Реализация исторического (подстановочного или перестановочного) шифра	4	2
2	Криптоанализ исторического шифра	4	2
3	Реализация симметричного блокового шифра	4	2
4	Реализация потокового генератора	4	2
Семестр 6			
5	Реализация системы с открытым ключом	3	3
6	Реализация атаки на систему с открытым ключом	3	3
7	Реализация ЭЦП	4	3
8	Реализация криптографического протокола по управлению ключами	4	4
9	Реализация специального криптографического протокола	4	4

Всего:	34	

4.5. Курсовое проектирование (работа)

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 6.

Таблица 6 Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 5, час	Семестр 6, час
1	2	3	4
Самостоятельная работа, всего	95	57	38
изучение теоретического материала дисциплины (ТО)	80	50	30
Подготовка к текущему контролю (ТК)	15	7	8

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. 8-10.

6. Перечень основной и дополнительной литературы

6.1. Основная литература

Перечень основной литературы приведен в таблице 7.

Таблица 7 – Перечень основной литературы

Шифр	Библиографическая ссылка / URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004.4 К 84	Крук, Е. А. Методы программирования и прикладные алгоритмы [Текст]: учебное пособие в 3 ч. Ч. 1 / Е. А. Крук, А. А. Овчинников; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб.: Изд-во ГУАП, 2014. - 178 с.	40
Х М 48	Информационная безопасность и защита информации [Текст]: учебное пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков; ред. С. А Клейменов. - 5-е изд., стер. - М.: Академия, 2011. - 331 с.	25
	Глухов М. М., Круглов И. А., Пичкур А. Б., Черемушкин А. В. Введение в теоретико-числовые методы криптографии. Лань, 2011. http://e.lanbook.com/view/book/1540/	

6.2. Дополнительная литература

Перечень дополнительной литературы приведен в таблице 8.

Таблица 8 – Перечень дополнительной литературы

Шифр	Библиографическая ссылка/ URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004.056.55 Е 78	Ерош, И. Л. Криптография. Первое знакомство: учебное пособие/ СПб.:ГОУ ВПО "СПбГУАП", 2008. - 84 с.	323
004.05 В 75	Воронов, А. В., Волошина Н.В. Основы защиты информации: учебное пособие. СПб.: ГОУ ВПО "СПбГУАП", 2009. - 78 с.	74
004.056.55(075) Б 70	Блоковые шифры: Учебное пособие/ С. В. Беззатеев, Е. А. Крук, А.А. Овчинников, В. Б. Прохорова; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб.: РИО ГУАП, 2003. - 63 с.	49
	Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. Handbook of Applied Cryptography http://cacr.uwaterloo.ca/hac/	

7. Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

URL адрес	Наименование
https://www.pgpru.com/	Проект "OpenPGP в России"

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

8.1. Перечень программного обеспечения

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10 – Перечень программного обеспечения

№ п/п	Наименование
1	Программный комплекс PGP
2	Менеджер паролей KeePass

8.2. Перечень информационно-справочных систем

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11 – Перечень информационно-справочных систем

№ п/п	Наименование
1	http://libgost.ru/ Библиотека ГОСТов и нормативных документов

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

Состав материально-технической базы представлен в таблице 12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Фонд аудиторий ГУАП для проведения занятий лекционного и семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	
2	Вычислительная лаборатория	

10. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

10.1. Состав фонда оценочных средств приведен в таблице 13

Таблица 13 - Состав фонда оценочных средств для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных средств
Экзамен	Список вопросов к экзамену
Зачет	Список вопросов

10.2. Перечень компетенций, относящихся к дисциплине, и этапы их формирования в процессе освоения образовательной программы приведены в таблице 14.

Таблица 14 – Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Номер семестра	Этапы формирования компетенций по дисциплинам/практикам в процессе освоения ОП
ОПК-2 «способность применять соответствующий математический аппарат для решения профессиональных задач»	
1	Математическая логика и теория алгоритмов
1	Математика. Математический анализ
1	Математика. Аналитическая геометрия и линейная алгебра
2	Дискретная математика
2	Математика. Аналитическая геометрия и линейная алгебра
2	Математика. Математический анализ
3	Математика. Теория вероятностей и математическая статистика
4	Алгоритмические проблемы криптографии
5	Теория информации
5	Криптографические методы защиты информации
6	Криптографические методы защиты информации
6	Моделирование информационных систем
6	Теория кодирования
ПК-1 «способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических	

средств защиты информации»	
4	Методы и средства защиты информации
4	Алгоритмические проблемы криптографии
5	Криптографические методы защиты информации
6	Криптографические методы защиты информации
6	Программно-аппаратные средства защиты информации
7	Программно-аппаратные средства защиты информации
7	Техническая защита информации
ПК-12 «способность принимать участие в проведении экспериментальных исследований системы защиты информации»	
5	Криптографические методы защиты информации
6	Криптографические методы защиты информации
8	Учебно-исследовательская работа студента
8	Производственная преддипломная практика

10.3. В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала модульно–рейтинговой системы университета. В таблице 15 представлена 100–балльная и 4-балльная шкалы для оценки сформированности компетенций.

Таблица 15 –Критерии оценки уровня сформированности компетенций

Оценка компетенции		Характеристика сформированных компетенций
100-балльная шкала	4-балльная шкала	
$85 \le К \le 100$	«отлично» «зачтено»	- обучающийся глубоко и всесторонне усвоил программный материал; - уверенно, логично, последовательно и грамотно его излагает; - опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; - умело обосновывает и аргументирует выдвигаемые им идеи; - делает выводы и обобщения; - свободно владеет системой специализированных понятий.
$70 \le К \le 84$	«хорошо» «зачтено»	- обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; - не допускает существенных неточностей; - увязывает усвоенные знания с практической деятельностью направления; - аргументирует научные положения; - делает выводы и обобщения; - владеет системой специализированных понятий.
$55 \le К \le 69$	«удовлетво-рительно» «зачтено»	- обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; - допускает несущественные ошибки и неточности; - испытывает затруднения в практическом применении знаний направления; - слабо аргументирует научные положения; - затрудняется в формулировании выводов и обобщений; - частично владеет системой специализированных понятий.

$К \leq 54$	«неудовлетворительно» «не зачтено»	- обучающийся не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - не формулирует выводов и обобщений.

10.4. Типовые контрольные задания или иные материалы:

1. Вопросы (задачи) для экзамена (таблица 16)

Таблица 16 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена
1	Задача обеспечения секретности.
2	Шифры подстановок. Примеры.
3	Шифры перестановок. Примеры.
4	Стойкость шифров. Модели атакующего
5	Симметричные блоковые шифры. Свойства, принципы построения.
6	Итеративные блоковые шифры. Сети Файстеля. Примеры.
7	Шифр DES.
8	Шифр ГОСТ 28147-89.
9	Шифр FEAL
10	Шифр IDEA.
11	Шифр AES.
12	Режимы блокового шифрования.
13	Регистры сдвига с линейной обратной связью. Алгоритм Берлекэмпа-Мэсси.
14	Потоковые шифры. Свойства, принципы построения.
15	Хэш-функции, свойства, принципы построения. MDC, MAC
16	Задача идентификации. Парольная идентификация
17	Асимметричные шифры. Свойства, принципы построения.
18	Система RSA.
19	Система Эль-Гамаля
20	Система Меркли-Хеллмана
21	Система Мак-Элиса
22	Задача обеспечения аутентификации. Цифровая подпись.
23	Подпись RSA.
24	Подпись DSA
25	Подпись Эль-Гамаля.
26	Подпись ГОСТ Р 34.10-94
27	Распределение ключей. Протокол Диффи-Хеллмана. Цифровой конверт
28	Распределение ключей. Сертификаты.

2. Вопросы (задачи) для зачета / дифференцированного зачета (таблица 17)

Таблица 17 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
1	Задача обеспечения секретности.
2	Шифры подстановок. Примеры.
3	Шифры перестановок. Примеры.
4	Стойкость шифров. Модели атакующего
5	Симметричные блоковые шифры. Свойства, принципы построения.
6	Итеративные блоковые шифры. Сети Файстеля. Примеры.
7	Шифр DES.

8	Шифр ГОСТ 28147-89.
9	Шифр FEAL
10	Шифр IDEA.
11	Шифр AES.
12	Режимы блокового шифрования.

3. Темы и задание для выполнения курсовой работы / выполнения курсового проекта (таблица 18)

Таблица 18 – Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта

№ п/п	Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта
	Учебным планом не предусмотрено

4. Вопросы для проведения промежуточной аттестации при тестировании (таблица 19)

Таблица 19 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
	Учебным планом не предусмотрено

5. Контрольные и практические задачи / задания по дисциплине (таблица 20)

Таблица 20 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
1	Задание 1. Основы модульной арифметики (50 вариантов) Пример задания: Вариант 1. Вычислить: -17 mod 44 -31 mod 17 -49 mod 16 -76 mod 11 23 mod 50
2	Задание 2. Нахождение мультипликативных обратных с помощью алгоритма Евклида (50 вариантов) Пример задания: Вариант 1. Вычислить: 1 8011 mod16732
3	Задание 3. Быстрое возведение в степень (50 вариантов) Пример задания: Вариант 1. Вычислить: 19220 mod73
4	Задание 4. Системы с открытым ключом: системы RSA, Мак-Элиса, Эль-Гамаля (индивидуальные варианты) Пример задания: Построить открытый и секретный ключи, зашифровать и расшифровать сообщение с помощью системы Мак-Элиса, для сообщения m = 100101. Параметр M определяется индивидуальным номером студента, остальные параметры системы выбрать самостоятельно.
5	Задание 5. Системы ЭЦП: системы RSA, Эль-Гамаля (индивидуальные варианты) Пример задания:

	Построить открытый и секретный ключи, подписать и проверить подпись сообщения с помощью системы Эль-Гамаля. Сообщение М определяется индивидуальным номером студента, размер открытого модуля p > 19, остальные параметры ЭЦП выбрать самостоятельно.

10.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и / или опыта деятельности, характеризующих этапы формирования компетенций, содержатся в Положениях «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

11. Методические указания для обучающихся по освоению дисциплины

Цель дисциплины - научить студентов понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности.

Методические указания для обучающихся по освоению лекционного материала

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемые результаты при освоении обучающимся лекционного материала:

– получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;

– получение опыта творческой работы совместно с преподавателем;

– развитие профессионально–деловых качеств, любви к предмету и самостоятельного творческого мышления.

– появление необходимого интереса, необходимого для самостоятельной работы;

– получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;

– научится методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);

– получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала:

Раздел 1. Основные понятия криптографии

Тема 1.1. Основные определения

Тема 1.2. Задачи информационной безопасности

Раздел 2. Симметричные шифры

Тема 2.1 Исторические шифры

Тема 2.2 Блоковые шифры

Тема 2.3 Потоковые шифры

Раздел 3. Криптография с открытым ключом
Тема 3.1 Математические основы систем с открытым ключом
Тема 3.2 Основные алгоритмы с открытым ключом
Раздел 4. Криптографические протоколы
Тема 4.1 Основные протоколы с открытым ключом
Тема 4.2 Специальные протоколы

Методические указания для обучающихся по прохождению лабораторных работ

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом, и относится к средствам, обеспечивающим решение следующих основных задач у обучающегося:

– приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;
– закрепление, развитие и детализация теоретических знаний, полученных на лекциях;
– получение новой информации по изучаемой дисциплине;
– приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание и требования к проведению лабораторных работ

Вариант задания по каждой лабораторной работе обучающийся получает в соответствии с номером в списке группы. Перед проведением лабораторной работы обучающемуся следует внимательно ознакомиться с методическими указаниями по ее выполнению, а также с содержанием соответствующего лекционного курса, при необходимости – изучить самостоятельно дополнительную литературу. В соответствии с заданием обучающийся должен подготовить необходимые данные, выполнить задание лабораторной работы, получить требуемые результаты, оформить и защитить отчет по лабораторной работе.

Структура и форма отчета о лабораторной работе

Отчет о лабораторной работе должен включать в себя: титульный лист, формулировку задания, теоретические положения, используемые при выполнении лабораторной работы, описание процесса выполнения лабораторной работы, полученные результаты и выводы.

Требования к оформлению отчета о лабораторной работе

По каждой лабораторной работе выполняется отдельный отчет. Титульный лист оформляется в соответствии с шаблоном (образцом) приведенным на сайте ГУАП (www.guap.ru) в разделе «Сектор нормативной документации». Текстовые и графические материалы оформляются в соответствии с действующими ГОСТами и требованиями, приведенными на сайте ГУАП (www.guap.ru) в разделе «Сектор нормативной документации».

Методические указания для выполнения лабораторных работ:

Овчинников А.А. Криптографические методы: методические указания для выполнения лабораторных работ по дисциплине «Криптографические методы защиты информации». Электронный ресурс кафедры №51.

[519.6/.8 Д 48] Дискретная математика. Задачи и контрольные работы по теории чисел [Текст]: методические указания / С.-Петерб. гос. ун-т аэрокосм. приборостроения; сост. С.В. Федоренко. - СПб.: Изд-во ГУАП, 2011. - 19 с. (78 экз.)

[519.6./8 Д 48] Дискретная математика. Основные понятия теории чисел [Текст]: методические указания / С.-Петерб. гос. ун-т аэрокосм. приборостроения; сост. С.В. Федоренко. - СПб.: Изд-во ГУАП, 2011. - 16 с. (77 экз.)

[519.6./8 Д 48] Дискретная математика. Дополнительные главы теории чисел [Текст]: методические указания / С.-Петерб. гос. ун-т аэрокосм. приборостроения ; сост. С.В. Федоренко. - СПб.: Изд-во ГУАП, 2011. - 15 с. (77 экз.)

Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

В процессе выполнения самостоятельной работы, у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет им развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихся является учебно-методический материал по дисциплине.

Для развития у студентов навыков самостоятельного овладения теоретическим материалом ряд тем дисциплины на лекционных занятиях дается обзорно, что предполагает их самостоятельное детальное изучение.

Примерные темы для самостоятельного изучения:

1. Метод тотального опробования ключей. Определение числа ключей в ряде конкретных схем шифраторов.
2. Протоколы цифровых денег
3. Роторные машины.
4. Многократное шифрование.
5. Методы построения больших периодов в поточных шифрах.
6. m-последовательности.
7. Нелинейное комбинирование РСЛОС
8. Методы целочисленной факторизации
9. Методы вычисления дискретных логарифмов
10. Постквантовая криптография
11. Доказательства с нулевым разглашением
12. Защищенные распределенные вычисления
13. Методы анализа хэш-функций. Вычисление вероятностей коллизий

Методические указания для обучающихся по прохождению промежуточной аттестации

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

– экзамен – форма оценки знаний, полученных обучающимся в процессе изучения всей дисциплины или ее части, навыков самостоятельной работы, способности применять их для решения практических задач. Экзамен, как правило, проводится в период экзаменационной сессии и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

– зачет – это форма оценки знаний, полученных обучающимся в ходе изучения учебной дисциплины в целом или промежуточная (по окончании семестра) оценка знаний обучающимся по отдельным разделам дисциплины с аттестационной оценкой «зачтено» или «не зачтено».

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой