

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

Кафедра № 33

УТВЕРЖДАЮ

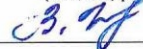
Руководитель образовательной программы

ДОЦ., К.Т.Н.

(должность, уч. степень, звание)

В.И. Казаков

(инициалы, фамилия)



(подпись)

«19» февраля 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Постквантовая обработка»  
(Наименование дисциплины)

|                                                       |                                        |
|-------------------------------------------------------|----------------------------------------|
| Код направления подготовки/<br>специальности          | 12.03.05                               |
| Наименование направления<br>подготовки/ специальности | Лазерная техника и лазерные технологии |
| Наименование<br>направленности                        | Лазерная техника и лазерные технологии |
| Форма обучения                                        | очная                                  |
| Год приема                                            | 2024                                   |

Лист согласования рабочей программы дисциплины

Программу составил (а)

Д.Т.Н., доц.

(должность, уч. степень, звание)

19.02.2025

(подпись, дата)

С.В. Беззатеев

(инициалы, фамилия)

Программа одобрена на заседании кафедры № 33

«19» февраля 2025 г, протокол № 7

Заведующий кафедрой № 33

Д.Т.Н., доц.

(уч. степень, звание)

19.02.2025

(подпись, дата)

С.В. Беззатеев

(инициалы, фамилия)

Заместитель директора института №2 по методической работе

доц., К.Т.Н., доц.

(должность, уч. степень, звание)

19.02.2025

(подпись, дата)

Н.В. Марковская

(инициалы, фамилия)

## Аннотация

Дисциплина «Постквантовая обработка» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 12.03.05 «Лазерная техника и лазерные технологии» направленности «Лазерная техника и лазерные технологии». Дисциплина реализуется кафедрой «№33».

Дисциплина не является обязательной при освоении обучающимся образовательной программы и направлена на углубленное формирование следующих компетенций:

ПК-6 «Квантовые технологии»

Содержание дисциплины охватывает круг вопросов, связанных с основными принципами и методами, применяемыми при синтезе и анализе криптосистем.

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 зачета.

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа.

Язык обучения по дисциплине «русский»

## 1. Перечень планируемых результатов обучения по дисциплине

### 1.1. Цели преподавания дисциплины

Получение обучающимися необходимых знаний и навыков в области вопросов, связанных с методами шифрования, используемыми в постквантовой криптографии, NP-сложными задачами, направлениями постквантовой криптографии, кодами, исправляющими ошибки, атаками на систему МакЭлиса.

1.2. Дисциплина является факультативной дисциплиной по направлению образовательной программы высшего образования (далее – ОП ВО).

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

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями или их частями. Компетенции и индикаторы их достижения приведены в таблице 1.

Таблица 1 – Перечень компетенций и индикаторов их достижения

| Категория (группа) компетенции | Код и наименование компетенции | Код и наименование индикатора достижения компетенции                                                                                                                                                 |
|--------------------------------|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Профессиональные компетенции   | ПК-6 Квантовые технологии      | ПК-6.3.1 знать принципы работы и построения систем квантовой криптографии и квантовых вычислений<br>ПК-6.У.1 уметь настраивать системы квантовой криптографии, выявлять неисправность и устранять ее |

## 2. Место дисциплины в структуре ОП

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

- «Теория информации»,
- «Методы моделирования и оптимизации»

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и могут использоваться при написании выпускной квалификационной работы.

## 3. Объем и трудоемкость дисциплины

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 2.

Таблица 2 – Объем и трудоемкость дисциплины

| Вид учебной работы                              | Всего | Трудоемкость по семестрам |
|-------------------------------------------------|-------|---------------------------|
|                                                 |       | №6                        |
| 1                                               | 2     | 3                         |
| <b>Общая трудоемкость дисциплины, ЗЕ/ (час)</b> | 2/ 72 | 2/ 72                     |
| <b>Из них часов практической подготовки</b>     | 17    | 17                        |
| <b>Аудиторные занятия, всего час.</b>           | 34    | 34                        |
| в том числе:                                    |       |                           |
| лекции (Л), (час)                               | 17    | 17                        |
| практические/семинарские занятия (ПЗ), (час)    | 17    | 17                        |
| лабораторные работы (ЛР), (час)                 |       |                           |

|                                                                                             |       |       |
|---------------------------------------------------------------------------------------------|-------|-------|
| курсовой проект (работа) (КП, КР), (час)                                                    |       |       |
| экзамен, (час)                                                                              |       |       |
| <b>Самостоятельная работа</b> , всего (час)                                                 | 38    | 38    |
| <b>Вид промежуточной аттестации:</b> зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**) | Зачет | Зачет |

Примечание: \*\* кандидатский экзамен

#### 4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий.

Разделы, темы дисциплины и их трудоемкость приведены в таблице 3.

Таблица 3 – Разделы, темы дисциплины, их трудоемкость

| Разделы, темы дисциплины                                                                                                                                    | Лекции<br>(час) | ПЗ (СЗ)<br>(час) | ЛР<br>(час) | КП<br>(час) | СРС<br>(час) |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|------------------|-------------|-------------|--------------|
| <b>Семестр 3</b>                                                                                                                                            |                 |                  |             |             |              |
| Раздел 1. Введение                                                                                                                                          | 1               |                  |             |             | 8            |
| Раздел 2. Элементы теории NP-полных задач и задача анализа стойкости криптографических систем.<br>Тема 2.1. – Основные понятия. Тема 2.2. - Класс задач NP. | 4               |                  | 4           |             | 8            |
| Раздел 3. Принципы криптоанализа.<br>Тема 3.1. – Анализ стойкости систем.<br>Тема 3.2. – Криптоанализ ранцевых систем.                                      | 5               |                  | 4           |             | 8            |
| Раздел 4. Кодовые криптосистемы.<br>Тема 4.1. – Основные понятия теории кодирования.<br>Тема 4.2. – Традиционные кодовые криптосистемы.                     | 7               |                  | 9           |             | 14           |
| Итого в семестре:                                                                                                                                           | 17              |                  | 17          |             | 38           |
| Итого                                                                                                                                                       | 17              | 0                | 17          | 0           | 38           |
|                                                                                                                                                             |                 |                  |             |             |              |

Практическая подготовка заключается в непосредственном выполнении обучающимися определенных трудовых функций, связанных с будущей профессиональной деятельностью.

4.2. Содержание разделов и тем лекционных занятий.

Содержание разделов и тем лекционных занятий приведено в таблице 4.

Таблица 4 – Содержание разделов и тем лекционного цикла

| Номер раздела | Название и содержание разделов и тем лекционных занятий                                                                                                                                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1</b>      | Раздел 1. Введение<br>Классификация криптографических систем                                                                                                                                                                                                                                    |
| <b>2</b>      | Раздел 2. Элементы теории NP-полных задач и задача анализа стойкости криптографических систем.<br>Тема 2.1. – Основные понятия.<br>Детерминированные машины Тьюринга и класс задач P. Тема 2.2. - Класс задач NP.<br>Недетерминированные алгоритмы и класс задач NP. Основные NP-полные задачи. |

|          |                                                                                                                                                                                                                                                                                                                                    |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>3</b> | Раздел 3. Принципы криптоанализа. Тема 3.1. – Анализ стойкости систем.<br>Прямая и косвенная атаки на криптографические системы. Тема 3.2. – Криптоанализ ранцевых систем.<br>Атака Шамира ранцевых систем. Криптоатака Лагариса-Одлыжко.                                                                                          |
| <b>4</b> | Раздел 4. Кодовые криптосистемы.<br>Тема 4.1. – Основные понятия теории кодирования. NP-полные задачи кодирования.<br>Тема 4.2. – Традиционные кодовые криптосистемы. Атака системы Мак-Элиса, основанная на анализе группы симметрии кода. Системы, основанные на задаче полного декодирования. Модификации кодовых криптосистем. |

#### 4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Практические занятия и их трудоемкость

| № п/п     | Темы практических занятий               | Формы практических занятий | Трудоемкость, (час) | Из них практической подготовки, (час) | № раздела дисциплины |
|-----------|-----------------------------------------|----------------------------|---------------------|---------------------------------------|----------------------|
| Семестр 6 |                                         |                            |                     |                                       |                      |
| 1         | Машина Тьюринга                         | Решение задач              | 2                   |                                       | 2                    |
| 2         | Задача о сумме подмножества             | Решение задач              | 2                   |                                       | 2                    |
| 3         | Факторизация целых чисел                | Решение задач              | 2                   |                                       | 3                    |
| 4         | Вычисление дискретного логарифма        | Решение задач              | 2                   |                                       | 3                    |
| 5         | Декодирование линейного кода            | Решение задач              | 3                   |                                       | 4                    |
| 6         | Оценка параметров кодовой криптосистемы | Решение задач              | 3                   |                                       | 4                    |
| 7         | Модификации кодовых криптосистем        | Решение задач              | 3                   |                                       | 4                    |
| Всего     |                                         |                            | 17                  |                                       |                      |

#### 4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 6.

Таблица 6 – Лабораторные занятия и их трудоемкость

| № п/п                           | Наименование лабораторных работ | Трудоемкость, (час) | Из них практической подготовки, (час) | № раздела дисциплины |
|---------------------------------|---------------------------------|---------------------|---------------------------------------|----------------------|
| Учебным планом не предусмотрено |                                 |                     |                                       |                      |
|                                 |                                 |                     |                                       |                      |
| Всего                           |                                 |                     |                                       |                      |

#### 4.5. Курсовое проектирование/ выполнение курсовой работы

Учебным планом не предусмотрено

#### 4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

| Вид самостоятельной работы                        | Всего,<br>час | Семестр 6,<br>час |
|---------------------------------------------------|---------------|-------------------|
| 1                                                 | 2             | 3                 |
| Изучение теоретического материала дисциплины (ТО) | 20            | 20                |
| Курсовое проектирование (КП, КР)                  |               |                   |
| Расчетно-графические задания (РГЗ)                |               |                   |
| Выполнение реферата (Р)                           |               |                   |
| Подготовка к текущему контролю успеваемости (ТКУ) | 8             | 8                 |
| Домашнее задание (ДЗ)                             |               |                   |
| Контрольные работы заочников (КРЗ)                |               |                   |
| Подготовка к промежуточной аттестации (ПА)        | 10            | 10                |
| Всего:                                            | 38            | 38                |

#### 5. Перечень учебно-методического обеспечения

для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. 7-11.

#### 6. Перечень печатных и электронных учебных изданий

Перечень печатных и электронных учебных изданий приведен в таблице 8.

Таблица 8– Перечень печатных и электронных учебных изданий

| Шифр/<br>URL адрес | Библиографическая ссылка                                                                                                                                                       | Количество экземпляров в библиотеке<br>(кроме электронных экземпляров) |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| 004<br>Р 98        | Рябко, Б. Я. Криптографические методы защиты информации [Текст]: учебное пособие / Б. Я. Рябко, А. Н. Фионов. - 2-е изд., стер. - М. : Горячая линия - Телеком, 2014. - 229 с. | 10                                                                     |
| 004<br>В 75        | Основы защиты информации. Защита персонального компьютера от умышленных угроз [Текст]: учебное пособие / А. В. Воронов, Ю. В. Трифонова; С.- Петерб. гос. ун-таэроком.         | 57                                                                     |
|                    | Трифопова; С.- Петерб. гос. ун-таэроком.                                                                                                                                       |                                                                        |

|                                                                                                             |                                                                                                                                                                                             |    |
|-------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
|                                                                                                             | приборостроения. - СПб.:Изд-во ГУАП, 2015. - 99 с.                                                                                                                                          |    |
| 004/М 87-604316-ED                                                                                          | Защищенные инфотелекоммуникации. Анализ и синтез: монография / Н. Н. Мошак; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Электрон. текстовые дан. - СПб. : Изд-во ГУАП, 2014. - 197 с. | 40 |
| <a href="http://znanium.com/catalog.php?bookinfo=427831">http://znanium.com/catalog.php?bookinfo=427831</a> | Основы современной криптографии и стеганографии / Рябко Б.Я., Фионов А.Н., 2-е изд. - М.: Гор. линия-Телеком, 2013. - 232 с.                                                                |    |

#### 7. Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

| URL адрес                                                   | Наименование              |
|-------------------------------------------------------------|---------------------------|
| <a href="https://www.pgpru.com/">https://www.pgpru.com/</a> | Проект "OpenPGP в России" |

#### 8. Перечень информационных технологий

8.1. Перечень программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине.

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

| № п/п | Наименование     |
|-------|------------------|
|       | Не предусмотрено |

8.2. Перечень информационно-справочных систем,используемых при осуществлении образовательного процесса по дисциплине

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

| № п/п | Наименование     |
|-------|------------------|
|       | Не предусмотрено |

#### 9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице12.

Таблица 12 – Состав материально-технической базы

| № п/п | Наименование составной части материально-технической базы | Номер аудитории (при необходимости) |
|-------|-----------------------------------------------------------|-------------------------------------|
|-------|-----------------------------------------------------------|-------------------------------------|

|   |                                     |  |
|---|-------------------------------------|--|
| 1 | Лекционная аудитория                |  |
| 2 | Мультимедийная лекционная аудитория |  |

#### 10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине приведен в таблице 13.

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

| Вид промежуточной аттестации | Перечень оценочных средств            |
|------------------------------|---------------------------------------|
| Зачет                        | Список вопросов;<br>Тесты;<br>Задачи. |

10.2. В качестве критериев оценки уровня сформированности (освоения) компетенций обучающимися применяется 5-балльная шкала оценки сформированности компетенций, которая приведена в таблице 14. В течение семестра может использоваться 100-балльная шкала модульно-рейтинговой системы Университета, правила использования которой, установлены соответствующим локальным нормативным актом ГУАП.

Таблица 14 – Критерии оценки уровня сформированности компетенций

| Оценка компетенции                    | Характеристика сформированных компетенций                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5-балльная шкала                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| «отлично»<br>«зачтено»                | <ul style="list-style-type: none"> <li>– обучающийся глубоко и всесторонне усвоил программный материал;</li> <li>– уверенно, логично, последовательно и грамотно его излагает;</li> <li>– опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления;</li> <li>– умело обосновывает и аргументирует выдвигаемые им идеи;</li> <li>– делает выводы и обобщения;</li> <li>– свободно владеет системой специализированных понятий.</li> </ul> |
| «хорошо»<br>«зачтено»                 | <ul style="list-style-type: none"> <li>– обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы;</li> <li>– не допускает существенных неточностей;</li> <li>– увязывает усвоенные знания с практической деятельностью направления;</li> <li>– аргументирует научные положения;</li> <li>– делает выводы и обобщения;</li> <li>– владеет системой специализированных понятий.</li> </ul>                                                                    |
| «удовлетворительно»<br>«зачтено»      | <ul style="list-style-type: none"> <li>– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы;</li> <li>– допускает несущественные ошибки и неточности;</li> <li>– испытывает затруднения в практическом применении знаний направления;</li> <li>– слабо аргументирует научные положения;</li> <li>– затрудняется в формулировании выводов и обобщений;</li> <li>– частично владеет системой специализированных понятий.</li> </ul>                 |
| «неудовлетворительно»<br>«не зачтено» | <ul style="list-style-type: none"> <li>– обучающийся не усвоил значительной части программного материала;</li> <li>– допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении;</li> <li>– испытывает трудности в практическом применении знаний;</li> <li>– не может аргументировать научные положения;</li> </ul>                                                                                                                                                                          |

|                    |                                           |
|--------------------|-------------------------------------------|
| Оценка компетенции | Характеристика сформированных компетенций |
| 5-балльная шкала   |                                           |
|                    | – не формулирует выводов и обобщений.     |

10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

| № п/п | Перечень вопросов (задач) для экзамена | Код индикатора |
|-------|----------------------------------------|----------------|
|       | Учебным планом не предусмотрено        |                |

Вопросы (задачи) для зачета / дифф. зачета представлены в таблице 16.

Таблица 16 – Вопросы (задачи) для зачета / дифф. зачета

| № п/п | Перечень вопросов (задач) для зачета / дифф. зачета                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Код индикатора |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| 1     | Классификация криптографических систем.<br>Симметричные и несимметричные криптографические функции.<br>Задачи криптоанализа.<br>Элементы теории NP-полных задач и задача анализа стойкости криптографических систем.<br>Задачи распознавания. Языки.<br>Детерминированные машины Тьюринга и класс задач P. Недетерминированные алгоритмы и класс задач NP.<br>Полиномиальная сводимость и NP-полные задачи.<br>Теорема Кука.<br>Основные NP-полные задачи.<br>Прямая и косвенная атаки на криптографические системы. Система Хеллмана-Меркля.<br>Теоретико-числовые криптосистемы и задача разложения чисел на простые множители. | ПК-6.3.1       |
| 2     | Атака Шамира ранцевых систем.<br>Модификации ранцевых систем и криптоатака Лагариса-Одлыжко.<br>Линейные коды. Способы задания.<br>Декодирование линейных кодов как «трудная» задача. Декодирование линейных кодов как «простая» задача. Системы Мак-Элиса и Нидеррайтера.<br>Прямая атака кодовых криптосистем. Атака Сидельникова-Шестакова.<br>Атака системы Мак-Элиса, основанная на анализе группы симметрии кода.<br>Системы, основанные на задаче полного декодирования. Атака Зоргера.<br>Модификации кодовых криптосистем.                                                                                               | ПК-6.У.1       |

Перечень тем для курсового проектирования/выполнения курсовой работы представлены в таблице 17.

Таблица 17 – Перечень тем для курсового проектирования/выполнения курсовой работы

| № п/п | Примерный перечень тем для курсового проектирования/выполнения курсовой работы |
|-------|--------------------------------------------------------------------------------|
|       | Учебным планом не предусмотрено                                                |

Вопросы для проведения промежуточной аттестации в виде тестирования представлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

| № п/п | Примерный перечень вопросов для тестов | Код индикатора |
|-------|----------------------------------------|----------------|
|       | Не предусмотрено                       |                |

Перечень тем контрольных работ по дисциплине обучающихся заочной формы обучения, представлены в таблице 19.

Таблица 19 – Перечень контрольных работ

| № п/п | Перечень контрольных работ |
|-------|----------------------------|
|       | Не предусмотрено           |

10.4. Методические материалы, определяющие процедуры оценивания индикаторов, характеризующих этапы формирования компетенций, содержатся в локальных нормативных актах ГУАП, регламентирующих порядок и процедуру проведения текущего контроля успеваемости и промежуточной аттестации обучающихся ГУАП.

## 11. Методические указания для обучающихся по освоению дисциплины

11.1. 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 обучающимися 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;
- научиться 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. Введение

Раздел 2. Элементы теории NP-полных задач и задача анализа стойкости криптографических систем.

Тема 2.1. – Основные понятия.

Тема 2.2. – Класс задач NP.

Раздел 3. Принципы криптоанализа. Тема

3.1. – Анализ стойкости систем.

Тема 3.2. – Криптоанализ ранцевых систем.

Раздел 4. Кодовые криптосистемы.

Тема 4.1. – Основные понятия теории кодирования. Тема 4.2. – Традиционные кодовые криптосистемы.

### 11.2. Методические указания для обучающихся по выполнению лабораторных работ

#### 11.1. Методические указания для обучающихся по выполнению 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 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](http://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](http://www.guap.ru)) в разделе «Сектор нормативной документации».

#### 11.3. 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.

Для обучающихся по заочной форме обучения, самостоятельная работа может включать в себя контрольную работу.

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 являются:

- учебно-методический материал по дисциплине;
- методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

#### 11.4. Методические указания для обучающихся по прохождению текущего контроля успеваемости.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины.

#### 11.5. Методические указания для обучающихся по прохождению промежуточной аттестации.

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

- 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».

Лист внесения изменений в рабочую программу дисциплины

| Дата внесения изменений и дополнений.<br>Подпись внесшего изменения | Содержание изменений и дополнений | Дата и № протокола заседания кафедры | Подпись зав. кафедрой |
|---------------------------------------------------------------------|-----------------------------------|--------------------------------------|-----------------------|
|                                                                     |                                   |                                      |                       |
|                                                                     |                                   |                                      |                       |
|                                                                     |                                   |                                      |                       |
|                                                                     |                                   |                                      |                       |
|                                                                     |                                   |                                      |                       |