

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

Кафедра № 33

УТВЕРЖДАЮ

Руководитель направления

ДОЦ., К.Т.Н., ДОЦ.

(должность, уч. степень, звание)

В.В. Перлюк

(инициалы, фамилия)



(подпись)

«22» июня 2023 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Защита информации»
(Наименование дисциплины)

| | |
|---|--|
| Код направления подготовки/ специальности | 12.03.01 |
| Наименование направления подготовки/ специальности | Приборостроение |
| Наименование направленности | Авиационные приборы и измерительно-вычислительные комплексы |
| Форма обучения | заочная |

Санкт-Петербург– 2022

Аннотация

Дисциплина «Защита информации» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 12.03.01 «Приборостроение» направленности «Авиационные приборы и измерительно-вычислительные комплексы». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ОПК-4 «Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности»

Содержание дисциплины охватывает круг вопросов, раскрывающих сущность и значение информационной безопасности и защиты информации, их места в системе национальной безопасности, определение теоретических, концептуальных, методологических и организационных основ обеспечения безопасности.

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

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

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

Язык обучения по дисциплине «русский»

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Дисциплина имеет своей целью: обеспечить выполнение требований, изложенных в федеральном государственном образовательном стандарте высшего профессионального образования. Изучение дисциплины направлено на формирование перечисленных ниже элементов профессиональных компетенций.

Также целями освоения дисциплины «Защита информации» являются раскрытие сущности и значения информационной безопасности и защиты информации, их места в системе национальной безопасности, определение теоретических, концептуальных, методологических и организационных основ обеспечения безопасности информации, классификация и характеристики составляющих информационной безопасности и защиты информации, установление взаимосвязи и логической организации входящих в них компонентов.

1.2. Дисциплина входит в состав обязательной части 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 |
|----------------------------------|---|--|
| Общепрофессиональные компетенции | ОПК-4 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности | ОПК-4.3.2 знать стандарты, нормативы и требования информационной безопасности ОПК-4.У.2 уметь соблюдать требования информационной безопасности при использовании современных информационных технологий и программного обеспечения |

2. Место дисциплины в структуре ОП

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

- Информатика
- Информационные технологии

Знания, полученные при изучении материала данной дисциплины, имеют самостоятельное значение.

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 |
|--------------------|-------|---------------------------|
| | | №8 |
| 1 | 2 | 3 |

| | | |
|---|--------|--------|
| Общая трудоемкость дисциплины, ЗЕ/ (час) | 5/ 180 | 5/ 180 |
| Из них часов практической подготовки | | |
| Аудиторные занятия, всего час. | 16 | 16 |
| в том числе: | | |
| лекции (Л), (час) | 8 | 8 |
| практические/семинарские занятия (ПЗ), (час) | | |
| лабораторные работы (ЛР), (час) | 8 | 8 |
| курсовой проект (работа) (КП, КР), (час) | | |
| экзамен, (час) | 9 | 9 |
| Самостоятельная работа, всего (час) | 155 | 155 |
| Вид промежуточной аттестации: зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**) | Экз. | Экз. |

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 (час) | ПЗ (СЗ) (час) | ЛР (час) | КП (час) | СРС (час) |
|---|-----------------|------------------|-------------|-------------|--------------|
| Семестр 7 | | | | | |
| Раздел 1. Введение | 1 | | | | 12 |
| Раздел 2. Сущность и понятие информационной безопасности | 1 | | | | 12 |
| Раздел 3. Значение информационной безопасности и ее место в системе национальной безопасности | 1 | | | | 21 |
| Раздел 4. Сущность и понятие защиты информации | 1 | | | | 22 |
| Раздел 5. Состав и классификация носителей защищаемой информации | 1 | | 2 | | 22 |
| Раздел 6. Понятие и структура угроз защищаемой информации | 1 | | 2 | | 22 |
| Раздел 7. Объекты защиты информации | 1 | | 2 | | 22 |
| Раздел 8. Классификация видов, методов и средств защиты информации | 1 | | 2 | | 22 |
| Итого в семестре: | 8 | | 8 | | 155 |
| Итого | 8 | | 8 | | 155 |
| | | | | | |

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 |
|---------------|---|
| 1 | <i>Раздел 1. Введение.</i> Предмет и задачи курса. Значение и место курса в подготовке |

| | |
|---|---|
| | <p>специалистов, по защите информации. Научная и учебная взаимосвязь курса с другими дисциплинами. Разделы и темы, их распределение по видам аудиторных занятий. Формы проведения семинарских занятий. Состав и методика самостоятельной работы студентов по изучению дисциплины. Формы проверки знаний. Анализ нормативных источников, научной и учебной литературы. Знания и умения студентов, которые должны быть получены в результате изучения курса.</p> |
| 2 | <p><i>Раздел 2. Сущность и понятие информационной безопасности</i> Становление и развитие понятия "информационная безопасность". Современные подходы к определению понятия. Сущность информационной безопасности. Объекты информационной безопасности. Связь информационной безопасности с информатизацией общества. Структура информационной безопасности. Определение понятия информационная безопасность".</p> |
| 3 | <p><i>Раздел 3. Значение информационной безопасности и ее место в системе национальной безопасности</i> Значение информационной, безопасности для субъектов информационных отношений. Связь между информационной безопасностью и безопасностью информации. Понятие и современная концепция национальной безопасности. Место информационной, безопасности, в системе национальной безопасности.</p> |
| 4 | <p><i>Раздел 4. Сущность и понятие защиты информации</i> Существующие подходы к содержательной части понятия "защита информации" и способы реализации содержательной части. Методологическая основа раскрытия сущности и определения понятия защиты информации. Формы выражения нарушения статуса информации. Обусловленность статуса информации ее уязвимостью. Понятие уязвимости информации. Формы проявления уязвимости информации. Виды уязвимости информации. Понятие "утечка информации". Соотношение форм и видов уязвимости информации. Содержательная часть понятия "защита информации". Способ реализации содержательной части защиты информации. Определение понятия "защита информации", его соотношение с понятием, сформулированным в ГОСТ Р 50922-96. "Защита информации. Основные термины и определения".</p> |
| 5 | <p><i>Раздел 5. Состав и классификация носителей защищаемой информации</i> Понятие носитель защищаемой информации". Соотношение между носителем и источником информации. Состав носителей защищаемой информации. Способы фиксирования информации в носителях. Виды отображения информации в носителях. Методы воспроизведения отображенной информации в носителях информации. Носители письменной, видовой, излучаемой информации. Посредованные носители защищаемой информации. Свойства и значение типов носителей защищаемой информации.</p> |
| 6 | <p><i>Раздел 6. Понятие и структура угроз защищаемой информации</i> Современные подходы к понятию угрозы защищаемой информации. Связь угрозы защищаемой информации с уязвимостью информации. Признаки и составляющие угрозы: явления, факторы, условия. Понятие угрозы защищаемой</p> |

| | |
|---|--|
| | информации. Структура явлений как сущностного выражения угрозы защищаемой информации. Структура факторов, создающих возможность дестабилизирующего воздействия на информацию. |
| 7 | <i>Раздел 7. Объекты защиты информации</i> Понятие объекта защиты. Носители информации как конечные объекты защиты. Особенности отдельных видов носителей как объектов защиты. Состав объектов хранения письменных и видовых носителей информации, подлежащих защите. Состав подлежащих защите технических средств отображения, обработки, хранения, воспроизведения передачи информации. Другие объекты защиты информации. Виды и способы дестабилизирующего воздействия на объекты защиты. |
| 8 | <i>Раздел 8. Классификация видов, методов и средств защиты информации</i> Виды защиты информации, сферы их действия. Классификация методов защиты информации. Универсальные методы защиты информации, область их применения. Области применения организационных, криптографических и инженерно-технических методов защиты информации. Понятие и классификация средств защиты информации. Назначение программных, криптографических и технических средств защиты. |

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 |
|---------------------------------|---------------------------|----------------------------|---------------------|---------------------------------------|----------------------|
| Учебным планом не предусмотрено | | | | | |
| Всего | | | | | |

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 |
|-----------|--|---------------------|---------------------------------------|----------------------|
| Семестр 7 | | | | |
| 1 | Исследование уязвимости информации | 4 | | 5 |
| 2 | Исследование видов уязвимости | 4 | | 6 |
| 3 | Исследование форм уязвимости | 4 | | 7 |
| 4 | Построение алгоритмов социальной инженерии и способы защиты от них | 5 | | 8 |
| Всего | | 17 | | |

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, час | Семестр 7, час |
|---|------------|----------------|
| 1 | 2 | 3 |
| Изучение теоретического материала дисциплины (ТО) | 100 | 100 |
| Курсовое проектирование (КП, КР) | | |
| Расчетно-графические задания (РГЗ) | | |
| Выполнение реферата (Р) | | |
| Подготовка к текущему контролю успеваемости (ТКУ) | 30 | 30 |
| Домашнее задание (ДЗ) | | |
| Контрольные работы заочников (КРЗ) | | |
| Подготовка к промежуточной аттестации (ПА) | 25 | 25 |
| Всего: | 155 | 155 |

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/ URL адрес | Библиографическая ссылка | Количество экземпляров в библиотеке (кроме электронных экземпляров) |
|-----------------------|--|---|
| 004.05В 75 | Воронов, А. В. Основы защиты информации: учебное пособие/ А. В. Воронов, Н. В. Волошина. - СПб.: ГОУ ВПО "СПбГУАП", 2009. - 78 с. | |
| 004 Ш 22 | Шаньгин, В. Ф. Информационная безопасность [Текст]: научно-популярная литература / В. Ф. Шаньгин. - М.: ДМК Пресс, 2014. - 702 с | |
| Х Я 47 | Яковец, Е. Н. Правовые основы обеспечения информационной безопасности Российской Федерации [Текст] : учебное пособие / Е. Н. Яковец. - М. : Юрлитинформ, 2010. - 336 с. | |
| | http://e.lanbook.com/books/element.php?pl1_id=3032 Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. | |

| | | |
|----------|--|------|
| | : ДМК Пресс, 2012. — 592 с | |
| 004 М 48 | Мельников, В. П. Защита информации [Текст] : учебник / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; ред. В. П. Мельников. - М. : Академия, 2014. - 304 с. | (5) |
| 004 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) |
| | http://e.lanbook.com/books/element.php?pl1_id=4959 Титов, А.А. Инженерно-техническая защита информации [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : ТУСУР (Томский государственный университет систем управления и радиоэлектроники), 2010. — 195 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 |
|---|---|
| http://www.intuit.ru/studies/courses/10/10/info | Владимир Галатенко. Основы информационной безопасности (курс лекций, с дистанционным обучением) |

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 таблице 12.

Таблица 12 – Состав материально-технической базы

| № п/п | Наименование составной части материально-технической базы | Номер аудитории (при необходимости) |
|-------|---|-------------------------------------|
| 1 | Лекционная аудитория | |
| 2 | Компьютерный класс | |

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 |
|------------------------------|---|
| Экзамен | Список вопросов к экзамену; Экзаменационные билеты; Задачи; Тесты. |

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» «зачтено» | <ul style="list-style-type: none"> – 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. |
| «хорошо» «зачтено» | <ul style="list-style-type: none"> – 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. |
| «удовлетворительно» «зачтено» | <ul style="list-style-type: none"> – 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. |

| | |
|---------------------------------------|---|
| Оценка компетенции | Характеристика сформированных компетенций |
| 5-балльная шкала | |
| «неудовлетворительно» «не зачтено» | <ul style="list-style-type: none"> – 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. |

10.3. 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 |
|-------|--|----------------|
| 1 | <p>Анализ нормативных источников, научной и учебной литературы</p> <p>Становление и развитие понятия "информационная безопасность"</p> <p>Соотношение между носителем и источником информации.</p> <p>Виды отображения информации в носителях</p> <p>Состав объектов хранения письменных и видовых носителей информации, подлежащих защите</p> <p>Место информационной, безопасности, в системе национальной безопасности</p> <p>Методологическая основа раскрытия сущности и определения понятия защиты информации.</p> | ОПК-4.3.2 |
| 2 | <p>Связь информационной безопасности с информатизацией общества</p> <p>Значение информационной, безопасности для субъектов информационных</p> <p>Понятие «носитель защищаемой информации»</p> <p>Современные подходы к определению понятия.</p> <p>Сущность информационной безопасности. Объекты информационной безопасности</p> <p>Современные подходы к понятию угрозы защищаемой информации</p> <p>Понятие угрозы защищаемой информации.</p> <p>Понятие объекта защиты</p> <p>Другие объекты защиты информации.</p> <p>Виды и способы дестабилизирующего воздействия на объекты защиты.</p> <p>Существующие подходы к содержательной части понятия "защита информации" и способы реализации содержательной части</p> <p>Понятие уязвимости информации</p> <p>Виды защиты информации, сферы их действия</p> <p>Классификация методов защиты информации</p> <p>Понятие и классификация средств защиты информации.</p> <p>Назначение программных, криптографических и технических средств защиты</p> | ОПК-4.У.2 |

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 |
| | Учебным планом не предусмотрено | |

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 |
|-------|---|----------------|
| | Виды и способы дестабилизирующего воздействия на объекты защиты. Существующие подходы к содержательной части понятия "защита информации" и способы реализации содержательной части Понятие уязвимости информации Виды защиты информации, сферы их действия Классификация методов защиты информации Понятие и классификация средств защиты информации. Назначение программных, криптографических и технических средств защиты | |

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

Таблица 19 – Перечень контрольных работ

| № п/п | Перечень контрольных работ |
|-------|--|
| | Тесты по теме - Информационная безопасность (защита информации) с ответами Правильный вариант ответа отмечен знаком + 1) К правовым методам, обеспечивающим информационную безопасность, относятся: - Разработка аппаратных средств обеспечения правовых данных - Разработка и установка во всех компьютерных правовых сетях журналов учета действий + Разработка и конкретизация правовых нормативных актов обеспечения безопасности 2) Основными источниками угроз информационной безопасности являются все указанное в списке: - Хищение жестких дисков, подключение к сети, инсайдерство + Перехват данных, хищение данных, изменение архитектуры системы - Хищение данных, подкуп системных администраторов, нарушение регламента работы 3) Виды информационной безопасности: + Персональная, корпоративная, государственная - Клиентская, серверная, сетевая - Локальная, глобальная, смешанная 4) Цели информационной безопасности – своевременное обнаружение, предупреждение: + несанкционированного доступа, воздействия в сети - инсайдерства в организации - чрезвычайных ситуаций 5) Основные объекты информационной безопасности: + Компьютерные сети, базы данных - Информационные системы, психологическое состояние пользователей - Бизнес-ориентированные, коммерческие системы 6) Основными рисками информационной безопасности являются: |

- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
- + Потеря, искажение, утечка информации
- 7) К основным принципам обеспечения информационной безопасности относятся:
 - + Экономической эффективности системы безопасности
 - Многоплатформенной реализации системы
 - Усиления защищенности всех звеньев системы
- 8) Основными субъектами информационной безопасности являются:
 - руководители, менеджеры, администраторы компаний
 - + органы права, государства, бизнеса
 - сетевые базы данных, фаерволлы
- 9) К основным функциям системы безопасности можно отнести все перечисленное:
 - + Установление регламента, аудит системы, выявление рисков
 - Установка новых офисных приложений, смена хостинг-компании
 - Внедрение аутентификации, проверки контактных данных пользователей
- тест 10) Принципом информационной безопасности является принцип недопущения:
 - + Неоправданных ограничений при работе в сети (системе)
 - Рисков безопасности сети, системы
 - Презумпции секретности
- 11) Принципом политики информационной безопасности является принцип:
 - + Невозможности миновать защитные средства сети (системы)
 - Усиления основного звена сети, системы
 - Полного блокирования доступа при риск-ситуациях
- 12) Принципом политики информационной безопасности является принцип:
 - + Усиления защищенности самого незащищенного звена сети (системы)
 - Перехода в безопасное состояние работы сети, системы
 - Полного доступа пользователей ко всем ресурсам сети, системы
- 13) Принципом политики информационной безопасности является принцип:
 - + Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
 - Одноуровневой защиты сети, системы
 - Совместимых, однотипных программно-технических средств сети, системы
- 14) К основным типам средств воздействия на компьютерную сеть относятся:
 - Компьютерный сбой
 - + Логические закладки («мины»)
 - Аварийное отключение питания
- 15) Когда получен спам по e-mail с приложенным файлом, следует:
 - Прочитать приложение, если оно не содержит ничего ценного – удалить
 - Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
 - + Удалить письмо с приложением, не раскрывая (не читая) его
- 16) Принцип Кирхгофа:
 - Секретность ключа определена секретностью открытого сообщения
 - Секретность информации определена скоростью передачи данных
 - + Секретность закрытого сообщения определяется секретностью ключа
- 17) ЭЦП – это:
 - Электронно-цифровой преобразователь
 - + Электронно-цифровая подпись
 - Электронно-цифровой процессор
- 18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
 - Покупка нелегального ПО
 - + Ошибки эксплуатации и неумышленного изменения режима работы системы
 - Сознательного внедрения сетевых вирусов
- 19) Наиболее распространены угрозы информационной безопасности сети:
 - Распределенный доступ клиент, отказ оборудования
 - Моральный износ сети, инсайдерство
 - + Сбой (отказ) оборудования, нелегальное копирование данных
- тест 20) Наиболее распространены средства воздействия на сеть офиса:

| |
|--|
| <ul style="list-style-type: none"> - Слабый график, информационный обман, вирусы в интернет + Вирусы в сети, логические мины (закладки), информационный перехват - Компьютерные сбои, изменение администрирования, топологии 21) Утечкой информации в системе называется ситуация, характеризуемая: <ul style="list-style-type: none"> + Потерей данных в системе - Изменением формы информации - Изменением содержания информации 22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются: <ul style="list-style-type: none"> + Целостность - Доступность - Актуальности 23) Угроза информационной системе (компьютерной сети) – это: <ul style="list-style-type: none"> + Вероятное событие - Детерминированное (всегда определенное) событие - Событие, происходящее периодически 24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется: <ul style="list-style-type: none"> - Регламентированной - Правовой + Защищаемой 25) Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке: <ul style="list-style-type: none"> + Программные, технические, организационные, технологические - Серверные, клиентские, спутниковые, наземные - Личные, корпоративные, социальные, национальные 26) Окончательно, ответственность за защищенность данных в компьютерной сети несет: <ul style="list-style-type: none"> + Владелец сети - Администратор сети - Пользователь сети 27) Политика безопасности в системе (сети) – это комплекс: <ul style="list-style-type: none"> + Руководств, требований обеспечения необходимого уровня безопасности - Инструкций, алгоритмов поведения пользователя в сети - Нормы информационного права, соблюдаемые в сети 28) Наиболее важным при реализации защитных мер политики безопасности является: <ul style="list-style-type: none"> - Аудит, анализ затрат на проведение защитных мер - Аудит, анализ безопасности + Аудит, анализ уязвимостей, риск-ситуаций |
|--|

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

Целью дисциплины является – получение студентами необходимых знаний, умений и навыков в области дискретной математики. Создание поддерживающей образовательной среды преподавания служит участие студентов в конференциях, видеоконференциях, участие в научно-исследовательской работах обучающей кафедры.

Данная дисциплина предоставляет возможность студентам развивать и продемонстрировать навыки, используя методы комбинаторики, теории графов и теории

автоматов, алгоритмическими процедурами решения задач оптимизации на дискретных структурах.

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;
- 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:

- Изложение лекционного материала;
- Представление теоретического материала преподавателем в виде слайдов;
- Освоение теоретического материала по практическим вопросам;
- Список вопросов по теме для самостоятельной работы студента (Табл.21).

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

- В задании должно быть четко сформулирована задача, выполняемая в ЛР;
- Описаны входные и выходные данные для проведения ЛР;
- ЛР должна выполняться на основе полученных теоретических знаниях;
- Выполнение ЛР должно осуществляться на основе методических указаний, предоставляемых преподавателем;
- ЛР должна выполняться в специализированном компьютерном классе и может быть доработана студентом в домашних условиях, если позволяет ПО;
- Итогом выполненной ЛР является отчет.

Структура и форма отчета о лабораторной работе

- Постановка задачи;
- Входные и выходные данные;
- Содержание этапов выполнения;
- Обоснование полученного результата (вывод);
- Список используемой литературы.

Требования к оформлению отчета о лабораторной работе

- Лабораторная работа (ЛР) предоставляется в печатном/или электронном виде;
 - ЛР должна соответствовать структуре и форме отчета представленной выше;
 - ЛР должна иметь титульный лист (ГОСТ 7.32-2001 издания 2008 года) с названием и подписью студента(ов), который(ые) ее сделал(и) и оформил(и);
- Студент должен защитить ЛР. Отметка о защите должна находиться на титульном листе вместе с подписью преподавателя.

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).

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».

– дифференцированный зачет – это форма оценки знаний, полученных обучающимся при изучении дисциплины, при выполнении курсовых проектов, курсовых работ, научно-исследовательских работ и прохождении практик с аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

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 |
|---|-----------------------------------|--------------------------------------|-----------------------|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |