

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ  
ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего  
образования  
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра № 33

УТВЕРЖДАЮ  
Руководитель кафедры  
д.т.н. к.т.н. д.т.н.  
И.К. Погомаров  
«26» мая 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы информатизации деятельности»  
(дисциплина)

|  |  |
|--|--|
| Есть ли программа (подготовка)<br>специальности      | 24.05.06   |
| Наименование направления<br>подготовки специальности | Системы управления деятельностью человека          |
| Наименование<br>специальности                        | Приборы системы управления, летательная аппаратура |
| Формы обучения                                       | очная  |

Санкт-Петербург - 2022

Лист из прилагаемой рабочей программы дисциплины

Программа составлена (по)

д.т.н. д.т.н.  
С.В. Белицкий

26.05.22  
С.В. Белицкий

С.В. Белицкий  
Специальность: Физика

Программа составлена на заседании кафедры № 33

«26» мая 2022 г., протокол № 10

Заседаний кафедры № 33

д.т.н. д.т.н.  
С.В. Белицкий

26.05.22  
С.В. Белицкий

С.В. Белицкий  
Специальность: Физика

Ответственный за СИ (05 24 01 06 01)

д.т.н. к.т.н. д.т.н.  
И.К. Погомаров

26.05.22  
И.К. Погомаров

И.К. Погомаров  
Специальность: Физика

Заседания: директор института №1 по учебно-методической работе

д.т.н. к.т.н. д.т.н.  
И.К. Погомаров

26.05.22  
И.К. Погомаров

И.К. Погомаров  
Специальность: Физика

## Аннотация

Дисциплина «Основы информационной безопасности» входит в образовательную программу высшего образования – программу специалитета по направлению подготовки/ специальности 24.05.06 «Системы управления летательными аппаратами» направленности «Приборы систем управления летательных аппаратов». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ОПК-2 «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, лабораторные работы, самостоятельная работа студента, консультации.

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

Общая трудоемкость освоения дисциплины составляет 4 зачетных единицы, 144 часа.

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 «Основы информационной безопасности» 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-2 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности | ОПК-2.3.1 знать современные информационные технологии для решения типовых задач профессиональной деятельности<br>ОПК-2.У.1 уметь применять программные средства для решения типовых задач профессиональной деятельности<br>ОПК-2.В.1 владеть навыками работы с современными программами в области компьютерной математики |

## 2. Место дисциплины в структуре ОП

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

- «Информатика»,
- «Основы теории информации»,
- «Основы программирования»

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

- «Производственная преддипломная практика»,
- «ГИА»

## 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 |
|---|--------|---------------------------|
|   |        | №7                        |
| 1   | 2      | 3                         |
| <b>Общая трудоемкость дисциплины, ЗЕ/ (час)</b>   | 4/ 144 | 4/ 144                    |
| <b>Из них часов практической подготовки</b>   |        |                           |
| <b>Аудиторные занятия, всего час.</b>   | 51     | 51                        |
| в том числе:  |        |                           |
| лекции (Л), (час)   | 34     | 34                        |
| практические/семинарские занятия (ПЗ), (час)  |        |                           |
| лабораторные работы (ЛР), (час)   | 17     | 17                        |
| курсовой проект (работа) (КП, КР), (час)  |        |                           |
| экзамен, (час)  | 36     | 36                        |
| <b>Самостоятельная работа, всего (час)</b>  | 57     | 57                        |
| <b>Вид промежуточной аттестации:</b> зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**) | Экз.   | Экз.                      |

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 (час) | ПЗ (СЗ) (час) | ЛР (час) | КП (час) | СРС (час) |
|---|--------------|---------------|----------|----------|-----------|
| Семестр 7   |              |               |          |          |           |
| Раздел 1. Введение. Цель и задачи курса   | 2            |               |          |          | 6         |
| Раздел 2. Сущность и понятие информационной безопасности                                      | 4            |               |          |          | 6         |
| Раздел 3. Значение информационной безопасности и ее место в системе национальной безопасности | 4            |               |          |          | 6         |
| Раздел 4. Сущность и понятие защиты информации  | 4            |               |          |          | 7         |
| Раздел 5. Состав и классификация носителей защищаемой информации                              | 4            |               | 4        |          | 8         |
| Раздел 6. Понятие и структура угроз защищаемой информации                                     | 4            |               | 4        |          | 8         |
| Раздел 7. Объекты защиты информации   | 4            |               | 4        |          | 8         |
| Раздел 8. Классификация видов, методов и средств защиты информации                            | 8            |               | 5        |          | 8         |
| Итого в семестре:   | 34           |               | 17       |          | 57        |
| Итого   | 34           | 0             | 17       | 0        | 57        |

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             | <p><i>Раздел 1. Введение.</i><br/>                     Предмет и задачи курса. Значение и место курса в, подготовке 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><br/>                     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><br/>                     Значение информационной, безопасности для субъектов информационных отношений.<br/>                     Связь между информационной безопасностью и безопасностью информации.<br/>                     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><br/>                     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.<br/>                     Понятие уязвимости информации. Формы проявления уязвимости информации. Виды уязвимости информации. Понятие "утечка информации". Соотношение форм и видов уязвимости информации. Содержательная часть понятия "защита информации".<br/>                     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><br/>                     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. Опосредованные носители защищаемой информации. Свойства и значение типов носителей защищаемой</p>   |

|   |  |
|---|--|
|   | информации.  |
| 6 | <i>Раздел 6. Понятие и структура угроз защищаемой информации</i><br>Современные подходы к понятию угрозы защищаемой информации. Связь угрозы защищаемой информации с уязвимостью информации. Признаки и составляющие угрозы: явления, факторы, условия. Понятие угрозы защищаемой 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><br>Понятие объекта защиты. Носители информации как конечные объекты защиты. Особенности отдельных видов носителей как объектов защиты.<br>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><br>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) | 30         | 30             |
| Курсовое проектирование (КП, КР)                  |            |                |
| Расчетно-графические задания (РГЗ)                |            |                |
| Выполнение реферата (Р)                           |            |                |
| Подготовка к текущему контролю успеваемости (ТКУ) | 10         | 10             |
| Домашнее задание (ДЗ)                             |            |                |
| Контрольные работы заочников (КРЗ)                |            |                |
| Подготовка к промежуточной аттестации (ПА)        | 17         | 17             |
| Всего:  | 57         | 57             |

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<br>адрес | Библиографическая ссылка  | Количество экземпляров в библиотеке<br>(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.   | 10   |
| 004 Ш 22              | Шаньгин, В. Ф.<br>Информационная безопасность [Текст]: научно-популярная литература / В. Ф. Шаньгин. - М.: ДМК Пресс, 2014. - 702 с | 10   |
| Х Я 47                | Яковец, Е. Н. Правовые основы обеспечения   | 5  |

|          |  |    |
|----------|--|----|
|          | информационной безопасности Российской Федерации [Текст] : учебное пособие / Е. Н. Яковец. - М. : Юрлитинформ, 2010. - 336 с.  |    |
|          | <a href="http://e.lanbook.com/books/element.php?pl1_id=3032">http://e.lanbook.com/books/element.php?pl1_id=3032</a><br>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.<br>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.<br>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 |
|          | <a href="http://e.lanbook.com/books/element.php?pl1_id=4959">http://e.lanbook.com/books/element.php?pl1_id=4959</a> 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  |
|---|---|
| <a href="http://www.intuit.ru/studies/courses/10/10/info">http://www.intuit.ru/studies/courses/10/10/info</a> | 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;<br>Экзаменационные билеты;<br>Задачи;<br>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<br>5-балльная шкала | Характеристика сформированных компетенций   |
|--|---|
| «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>  |

| Оценка компетенции                    | Характеристика сформированных компетенций   |
|---------------------------------------|---|
| 5-балльная шкала                      |   |
| «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> <li>– не формулирует выводов и обобщений.</li> </ul>   |

### 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>Математические модели формальной теории защиты информации.</p> <p>Стандарты в области защиты информации в вычислительной системе, «Оранжевая книга» США, российские стандарты.</p> <p>Криптографические методы защиты информации.</p> <p>Основные понятия криптографии.</p> <p>Исторические шифры.</p> <p>Теоретическая, практическая и временная стойкость системы криптографической защиты.</p> <p>Криптографические параметры узлов и блоков шифрующих автоматов.</p> <p>Методы получения псевдослучайных последовательностей.</p> <p>Генераторы псевдослучайных последовательностей и их свойства.</p> <p>Современные поточные и блочные алгоритмы шифрования.</p> <p>Системы асимметричного шифрования, открытый ключ, электронная подпись.</p> <p>Вопросы генерации и распределения ключей.</p> <p>Атаки на криптографические алгоритмы: алгоритмические, алгебраические, статистические.</p> <p>Методология обоснования надежности криптографической защиты.</p> <p>Криптографические протоколы с использованием симметричного и асимметричного шифрования.</p> <p>Криптографические протоколы с использованием цифровой подписи.</p> | ОПК-2.3.1      |

|   |   |           |
|---|---|-----------|
|   | <p>Криптографические протоколы генерации и распределения ключей.</p> <p>Протоколы разделения секрета и доказательства без разглашения.</p> <p>Протокол подбрасывания монеты по телефону.</p> <p>Оценка сложности арифметических операций.</p> <p>Непрерывные дроби и их свойства, квадратичные вычеты, асимптотический закон распределения простых чисел.</p> <p>Арифметические алгоритмы, (вычисление НОД, Символа Якоби), решение квадратных уравнений в конечных простых полях, алгоритмы построения и проверки простоты чисел, алгоритмы факторизации и дискретного логарифмирования.</p> <p>Криптосистема RSA, выбор параметров и взаимосвязь между ними.</p>  |           |
| 2 | <p>Методы и средства ограничения доступа к компонентам ЭВМ.</p> <p>Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.</p> <p>Методы и средства хранения ключевой информации.</p> <p>Средства обеспечения безопасности в ОС семейств Windows и UNIX, критерии защищенности ОС.</p> <p>Средства обеспечения безопасности в сетях.</p> <p>Протоколы аутентификации при удаленном доступе.</p> <p>Средства защиты серверов и рабочих станций.</p> <p>Средства защиты локальных сетей при подключении к Internet.</p> <p>Межсетевые экраны, электронные замки, криптофильтры, крипто роутеры.</p> <p>Области применения, достоинства, недостатки, реализуемые политики безопасности.</p> <p>Методы оценки качества применяемых средств защиты.</p> <p>Методы и средства защиты информации в СУБД.</p> <p>Средства идентификации и аутентификации, управление доступом, средства контроля, аудит безопасности.</p> | ОПК-2.У.1 |
| 3 | <p>Критерии защищенности БД и АИС.</p> <p>Методы и системы обнаружения компьютерных атак.</p> <p>Экспресс-анализ защищенности сетевого компьютера от удаленных атак через сеть.</p> <p>Перечень типовых угроз вычислительной системе со стороны потенциального злоумышленника.</p> <p>Основные принципы защиты вычислительной системы от несанкционированного доступа (проверка полномочий, разграничение доступа, аудит).</p> <p>Защита информации в локальных и глобальных вычислительных сетях и ее особенности.</p> <p>Роль и задачи администратора вычислительной системы и службы безопасности.</p>   | ОПК-2.В.1 |

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 |
|-------|---|----------------|
|       | <p>1) К правовым методам, обеспечивающим информационную безопасность, относятся:</p> <ul style="list-style-type: none"> <li>- Разработка аппаратных средств обеспечения правовых данных</li> <li>- Разработка и установка во всех компьютерных правовых сетях журналов учета действий</li> <li>+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности</li> </ul> <p>2) Основными источниками угроз информационной безопасности являются все указанное в списке:</p> <ul style="list-style-type: none"> <li>- Хищение жестких дисков, подключение к сети, инсайдерство</li> <li>+ Перехват данных, хищение данных, изменение архитектуры системы</li> <li>- Хищение данных, подкуп системных администраторов, нарушение регламента работы</li> </ul> <p>3) Виды информационной безопасности:</p> <ul style="list-style-type: none"> <li>+ Персональная, корпоративная, государственная</li> <li>- Клиентская, серверная, сетевая</li> <li>- Локальная, глобальная, смешанная</li> </ul> <p>4) Цели информационной безопасности – своевременное обнаружение, предупреждение:</p> <ul style="list-style-type: none"> <li>+ несанкционированного доступа, воздействия в сети</li> <li>- инсайдерства в организации</li> <li>- чрезвычайных ситуаций</li> </ul> <p>5) Основные объекты информационной безопасности:</p> <ul style="list-style-type: none"> <li>+ Компьютерные сети, базы данных</li> <li>- Информационные системы, психологическое состояние пользователей</li> <li>- Бизнес-ориентированные, коммерческие системы</li> </ul> <p>6) Основными рисками информационной безопасности являются:</p> <ul style="list-style-type: none"> <li>- Искажение, уменьшение объема, перекодировка информации</li> <li>- Техническое вмешательство, выведение из строя оборудования сети</li> <li>+ Потеря, искажение, утечка информации</li> </ul> <p>7) К основным принципам обеспечения информационной безопасности относится:</p> <ul style="list-style-type: none"> <li>+ Экономической эффективности системы безопасности</li> </ul> | ОПК-2.У.1      |

- 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-компания
  - 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 относится:
- 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:

- Слабый трафик, 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:

+ Потерей данных в системе

- Изменением формы информации

- Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

+ Целостность

- Доступность

- Актуальности

23) Угроза информационной системе (компьютерной сети) – это:

+ Вероятное событие

- Детерминированное (всегда определенное) событие

- Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

- Регламентированной

- Правовой

+ Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перечисленные в списке:

+ Программные, технические, организационные, технологические

- Серверные, клиентские, спутниковые, наземные

- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

+ Владелец сети

- Администратор сети

- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:

|  |  |  |
|--|--|--|
|  | + Руководств, требований обеспечения необходимого уровня безопасности<br>- Инструкций, алгоритмов поведения пользователя в сети<br>- Нормы информационного права, соблюдаемые в сети<br>28) Наиболее важным при реализации защитных мер политики безопасности является:<br>- Аудит, анализ затрат на проведение защитных мер<br>- Аудит, анализ безопасности<br>+ Аудит, анализ уязвимостей, риск-ситуаций |  |
|--|--|--|

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:

- Изложение лекционного материала;

- Представление теоретического материала преподавателем в виде слайдов;
- Освоение теоретического материала по практическим вопросам;
- Список вопросов по теме для самостоятельной работы студента

Методическое пособие кафедры для изучения курса Воронов, А. В. Основы защиты информации: учебное пособие/ А. В. Воронов, Н. В. Волошина. - СПб.: ГОУ ВПО "СПбГУАП", 2009. - 78 с.

#### 11.2. 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

- 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.



### 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 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».

Экзамен проводится в письменной форме и завершается оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение экзамена. На экзамен выделяется два академических часа.

Вопросы, выносимые на экзамен, список рекомендуемой литературы для подготовки к нему, критерии оценки результатов сдачи экзамена, а также порядок его проведения доводятся до сведения студентов не позднее, чем за две недели до сессии.

В период подготовки к экзамену обучающемуся рекомендуется подготовить обстоятельные ответы на все вопросы, используя рекомендуемую для подготовки литературу, а также посетить консультацию, проводимую перед экзаменом. Ответы обучающегося должны продемонстрировать глубокое и всестороннее усвоение учебного материала, уверенное, логичное, последовательное и грамотное его изложение, знание основной и дополнительной литературы.

Экзаменационные билеты для проведения экзамена формируются согласно списку вопросов, каждый билет включает три вопроса: два теоретических и одна задача.

Основными критериями оценки уровня подготовки и сформированности соответствующих компетенций студента при проведении экзамена в письменной форме являются:

- степень владения терминологией;
- уровень усвоения студентом теоретических знаний и умение использовать их для решения задач;
- ориентирование в нормативных правовых актах, научной и иной специальной литературе;
- логичность, обоснованность, четкость ответа;

- культура ответа.

Оценка «отлично» выставляется при условии выполнения следующих требований:

1) Студент демонстрирует:

- свободное владение терминологией;
- высокий уровень теоретических знаний и умение использовать их для решения задач;
- исчерпывающее последовательное, обоснованное и логически стройное изложение ответа, без ошибок;
- демонстрируют знание современной учебной и научной литературы;
- демонстрирует знания базовых нормативно-правовых актов;
- демонстрируют способность к анализу и сопоставлению различных подходов к решению заявленной в билете проблематики.

2) Студент без затруднений ориентируется в нормативных правовых актах, научной и иной специальной литературе.

3) Письменная речь студента грамотная, лаконичная, с правильной расстановкой акцентов.

Оценка «хорошо» выставляется при условии выполнения следующих требований:

1) Студент демонстрирует:

- владение терминологией на достаточном уровне;
- достаточный уровень теоретических знаний и умение использовать их для решения задач;
- грамотное и логичное изложение ответа, без существенных ошибок, но изложение недостаточно систематизировано и последовательно.

2) Студент с некоторыми затруднениями ориентируется в нормативных правовых актах, научной и иной специальной литературе.

3) Письменная речь студента грамотная, лаконичная, с правильной расстановкой акцентов.

Оценка «удовлетворительно» выставляется при условии выполнения следующих требований:

1) Студент демонстрирует:

- владение терминологией на минимальном уровне;
- низкий пороговый уровень теоретических знаний, усвоил только основной программный материал без знания отдельных особенностей;
- при ответе допускает неточности, материал недостаточно систематизирован;
- нарушения в последовательности изложения.

2) Студент с затруднениями ориентируется в нормативных правовых актах, научной и иной специальной литературе.

3) Письменная речь студента в основном грамотная, но не демонстрируется уверенное владение материалом.

Оценка «неудовлетворительно» выставляется при условии:

1) Студент не владеет профессиональной терминологией, демонстрирует низкий уровень теоретических знаний и умения использовать их для решения задач.

2) Студент не знает значительной части программного материала, допускает существенные грубые ошибки, не ориентируется в нормативных правовых актах, научной и иной специальной литературе.

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