МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Ивангородский гуманитарно-технический институт (филиал)
федерального государственного автономного образовательного учреждения высшего образования
"Санкт-Петербургский государственный университет аэрокосмического приборостроения"

Кафедра № 2

УТВЕРЖДАЮ
Ответственный за образовательную программу

старший преподаватель
(должность, уч. степень, звание)

А.А. Сорокин
(инициалы, фамилия)

(подпись)
«19» июня 2025 г

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы информационной безопасности»
(Наименование дисциплины)

| | |
|---|---|
| Код направления подготовки/ специальности | 15.03.04 |
| Наименование направления подготовки/ специальности | Автоматизация технологических процессов и производств |
| Наименование направленности | Автоматизация технологических процессов и производств |
| Форма обучения | очная |
| Год приема | |

Ивангород – 2025

Лист согласования рабочей программы дисциплины

Программу составил (а)

| доц.,к.т.н.,доц. | 19.06.2025 | А.В. Дагаев |
|---|---|---|
| (должность, уч. степень, звание) | (подпись, дата) | (инициалы, фамилия) |

Программа одобрена на заседании кафедры № 2
«19» июня 2025 г, протокол № 10

И.о. зав. кафедрой № 2

| д.ф.-м.н. | 19.06.2025 | Ю.В. Рождественский |
|---|---|---|
| (уч. степень, звание) | (подпись, дата) | (инициалы, фамилия) |

Заместитель директора ИФ ГУАП по методической работе

| | 19.06.2025 | Н.В. Шустер |
|---|---|---|
| (должность, уч. степень, звание) | (подпись, дата) | (инициалы, фамилия) |

Аннотация

Дисциплина «Основы информационной безопасности» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 15.03.04 «Автоматизация технологических процессов и производств» направленности «Автоматизация технологических процессов и производств. (ИФ)». Дисциплина реализуется кафедрой «№2».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ОПК-2 «Применять основные методы, способы и средства получения, хранения, переработки информации»

ОПК-6 «Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий»

Содержание дисциплины охватывает круг вопросов, связанных с сущностью и значением информации в развитии современного информационного общества, опасностями и угрозами, возникающими в этом процессе, соблюдением требований информационной безопасности.

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

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

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 Применять основные методы, способы и средства получения, хранения, переработки информации | ОПК-2.З.1 знать основные методы, способы и средства получения, хранения, переработки информации в рамках профессиональной деятельности<br>ОПК-2.У.1 уметь применять методы, способы и средства получения, хранения, переработки информации в рамках профессиональной деятельности<br>ОПК-2.В.1 владеть навыками работы с информацией в рамках профессиональной деятельности |
| Общепрофессиональные компетенции | ОПК-6 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий | ОПК-6.У.1 уметь решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности |

2. Место дисциплины в структуре ОП

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

– «Дискретная математика»;
– «Информатика»:
– «Информационные технологии»;
– «Производственная практика».

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

– «Планирование и технико-экономическое обоснование бизнес-проектов»;
– «Производственная преддипломная практика».

## 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 |
| ***Общая трудоемкость дисциплины***, ЗЕ/ (час) | 4/ 144 | 4/ 144 |
| ***Из них часов практической подготовки*** | | |
| ***Аудиторные занятия***, всего час. | 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) | | |
| ***Самостоятельная работа***, всего (час) | 93 | 93 |
| ***Вид промежуточной аттестации*:** зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**) | Дифф. Зач. | Дифф. Зач. |

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) | ЛР (час) | КП (час) | СРС (час) |
|---|---|---|---|---|---|
| Семестр 7 | | | | | |
| Раздел 1. Введение<br>Тема 1.1. Введение | 2 | 0 | 0 | 0 | 8 |
| Раздел 2. Информационная безопасность<br>Тема 2.1. Сущность и понятие информационной безопасности<br>Тема 2.2. Значение информационной безопасности и ее место в системе национальной безопасности | 8 | 0 | 0 | 0 | 16 |

| | | | | | |
|---|---|---|---|---|---|
| Раздел 3. Защита информации<br>Тема 3.1. Сущность и понятие защиты информации<br>Тема 3.2. Состав и классификация носителей защищаемой информации<br>Тема 3.3. Понятие и структура угроз защищаемой информации<br>Тема 3.4. Объекты защиты информации<br>Тема 3.5. Классификация видов, методов и средств защиты информации | 24 | 0 | 17 | 0 | 59 |
| Итого в семестре: | 34 | 0 | 17 | 0 | 93 |
| Итого | 34 | 0 | 17 | 0 | 93 |

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** | Введение<br>Тема 1.1. Введение.<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.<br>Анализ нормативных источников, научной и учебной литературы. Знания и умения студентов, которые должны быть получены в результате изучения курса. |
| **2** | Информационная безопасность<br>Тема 2.1. Сущность и понятие информационной безопасности 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".<br>Тема 2.2. Значение информационной безопасности и ее место в системе национальной безопасности<br>Значение информационной, безопасности для субъектов информационных отношений.<br>Связь между информационной безопасностью и безопасностью информации. |

| | |
|---|---|
| | Понятие и современная концепция национальной безопасности. Место информационной, безопасности, в системе национальной безопасности. |
| **3** | Защита информации<br>Тема 3.1. Сущность и понятие защиты информации<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".<br>Тема 3.2. Состав и классификация носителей защищаемой информации<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 информации.<br>Тема 3.3. Понятие и структура угроз защищаемой информации<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.<br>Тема 3.4. Объекты защиты информации<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.<br>Тема 3.5. Классификация видов, методов и средств защиты информации<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 | | | | | |

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 | 0 | 3 |
| 2 | Исследование видов уязвимости | 4 | 0 | 3 |
| 3 | Исследование форм уязвимости | 4 | 0 | 3 |
| 4 | Построение алгоритмов социальной инженерии | 3 | 0 | 3 |
| 5 | Способы защиты | 2 | 0 | 3 |
| 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) | 70 | 70 |
| Курсовое проектирование (КП, КР) | 0 | 0 |
| Расчетно-графические задания (РГЗ) | 0 | 0 |
| Выполнение реферата (Р) | 0 | 0 |
| Подготовка к текущему контролю успеваемости (ТКУ) | 13 | 13 |
| Домашнее задание (ДЗ) | 0 | 0 |
| Контрольные работы заочников (КРЗ) | 0 | 0 |
| Подготовка к промежуточной аттестации (ПА) | 10 | 10 |
| Всего: | 93 | 93 |

## 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) |
|---|---|---|
| https://znanium.ru/catalog/product/2082642 | Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2024. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2082642. – Режим доступа: по подписке. | - |
| https://znanium.ru/catalog/product/2140566 | Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, | - |

| | | |
|---|---|---|
| | А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2024. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2140566. – Режим доступа: по подписке. | |

## 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 |
|---|---|
| https://www.intuit.ru/ | Национальный Открытый Университет "ИНТУИТ" |
| https://elibrary.ru/ | eLIBRARY.RU - Научная электронная библиотека |
| http://lib.guap.ru/ | Библиотека ГУАП |
| https://znanium.com/ | Электронно-библиотечная система Znanium |
| https://urait.ru/ | Образовательная платформа Юрайт |

## 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 |
|---|---|
| 1. | Microsoft Office Professional Plus |
| 2. | Microsoft Windows 10 Professional |
| 3. | Microsoft Visio |
| 4. | Firefox |
| 5. | Acrobat Reader DC |
| 6. | Консультант Плюс |
| 7. | 7-Zip |
| 8. | CrypTool 2 |
| 9. | Gnu/Linux (Ubuntu) |
| 10. | OpenOffice |
| 11. | LibreOffice |

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 | Кабинет информационных технологий и программных систем для занятий лекционного типа, занятий практического типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, самостоятельной работы № 212<br>Основное оборудование:<br>стол преподавателя – 1 шт.<br>столы ученические – 18 шт.<br>стулья – 37 шт.<br>доска маркерная – 1 шт.<br>флипчарт – 1 шт.<br>интерактивная доска 4К – 1 шт.<br>Веб камера Logitech BCC950 ConferenceCam – 1 шт.<br>Пульт ДУ 960-000867 - 1шт.<br>ИБП Ippon Smart Winner 2000VA 1- шт<br>Компьютер Intel Compute BOXSTK1AW32SC – 1 шт<br>МФУ Sharp AR-5618 -1 шт<br>Планшет графический WACOM ONE M - 1шт<br>Принтер лазерный Kyocera FS-6970DN (1102J53EU0) - 1шт<br>Програмно аппаратный комплекс ASCOD GARANT - 1шт<br>Сервер ASCOD-Garant с комплектом рельсов для монтажа - 1шт<br>Роутер Mikro Tik RB2011UiAS-RM - 1шт<br>Коммутатор 16 port - 1 шт<br>Коммутатор 24 port - 1 шт<br>Клавиатура 15 - шт<br>Мышь 15 - шт<br>ПЭВМ– Core i3 8 ОЗУ 8GB, VGA 2GB – 12 шт<br>ПЭВМ– Core i5 16 ОЗУ 8GB, VGA 3060 16GB – 2 шт<br>Монитор – 12 шт<br>Монитор MS\|I 24” – 4 шт<br>Удлинитель HDMI GH-ERHD032 30m 1шт<br>Роутер wifi TP-LINK - 1 шт<br>Пульт для презентаций logitech - 1шт<br>Ноутбук 250 G4 - 1шт<br>Экран проекторный ELITE Screens - 1шт<br>Проектор BENQ MW526E DLP - 1шт<br>VR шлем PICO 4 128 GB Ultra – 2шт<br>Системный блок AM5 ryzen 7700/ 32 DDR5/ 4060 8 gb 2 шт | 212 |

| | | |
|---|---|---|
| | Монитор MSI 24 ”- 4 шт | |
| 2 | Помещения для организации самостоятельной работы № 111<br>Библиотека, читальный зал:<br>Мебель;<br>WiFi с выходом в вычислительную сеть ИФ ГУАП и Интернет, обеспечивающий доступ в электронную информационно-образовательную среду организации и к подписным ресурсам: Электронно-библиотечные системы «ZNANIUM», «Юрайт», «Лань»;<br>Оборудованные места для самостоятельной работы, зонированные офисными перегородками – 6шт.<br>Системный блок UNIVERSAL i3 D2 -8 шт<br>Монитор ACER V173Dob - 8 шт<br>Клавиатура 8 - шт<br>Мышь Genius PS/2 - 8 шт<br>МФУ Kyocera m2035dn - 2 шт<br>Коммутатор 8 port -2 шт | 111 |

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 |
|---|---|
| Дифференцированный зачёт | Список вопросов;<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» | – обучающийся глубоко и всесторонне усвоил программный материал;<br>– уверенно, логично, последовательно и грамотно его излагает;<br>– опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления;<br>– умело обосновывает и аргументирует выдвигаемые им идеи;<br>– делает выводы и обобщения;<br>– свободно владеет системой специализированных понятий. |
| «хорошо»<br>«зачтено» | – обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы;<br>– не допускает существенных неточностей;<br>– увязывает усвоенные знания с практической деятельностью направления;<br>– аргументирует научные положения;<br>– делает выводы и обобщения; |

| Оценка компетенции<br>5-балльная шкала | Характеристика сформированных компетенций |
|---|---|
| | – владеет системой специализированных понятий. |
| «удовлетворительно»<br>«зачтено» | – обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы;<br>– допускает несущественные ошибки и неточности;<br>– испытывает затруднения в практическом применении знаний направления;<br>– слабо аргументирует научные положения;<br>– затрудняется в формулировании выводов и обобщений;<br>– частично владеет системой специализированных понятий. |
| «неудовлетворительно»<br>«не зачтено» | – обучающийся не усвоил значительной части программного материала;<br>– допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении;<br>– испытывает трудности в практическом применении знаний;<br>– не может аргументировать научные положения;<br>– 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 | Становление и развитие понятия "информационная безопасность". Современные подходы к определению понятия. | ОПК-2.З.1 |
| 2 | Сущность информационной безопасности | ОПК-2.З.1 |
| 3 | Объекты информационной безопасности | ОПК-2.З.1 |
| 4 | Существующие подходы к содержательной части понятия "защита информации" и способы реализации содержательной части | ОПК-2.З.1 |
| 5 | Понятие уязвимости информации | ОПК-2.З.1 |
| 6 | Методологическая основа раскрытия сущности и определения понятия защиты информации | ОПК-2.З.1 |
| 7 | Понятие «носитель защищаемой информации» | ОПК-2.З.1 |
| 8 | Современные подходы к понятию угрозы защищаемой информации | ОПК-2.З.1 |
| 9 | Понятие угрозы защищаемой информации | ОПК-2.З.1 |
| 10 | Понятие объекта защиты | ОПК-2.З.1 |
| 11 | Связь информационной безопасности с информатизацией общества | ОПК-2.У.1 |
| 12 | Значение информационной, безопасности для субъектов информационных | ОПК-2.У.1 |

| | | |
|---|---|---|
| 13 | Место информационной, безопасности, в системе национальной безопасности | ОПК-2.У.1 |
| 14 | Соотношение между носителем и источником информации | ОПК-2.У.1 |
| 15 | Виды отображения информации в носителях | ОПК-2.У.1 |
| 16 | Состав объектов хранения письменных и видовых носителей информации, подлежащих защите | ОПК-2.В.1 |
| 17 | Другие объекты защиты информации | ОПК-2.В.1 |
| 18 | Виды и способы дестабилизирующего воздействия на объекты защиты | ОПК-2.В.1 |
| 19 | Виды защиты информации, сферы их действия | ОПК-2.В.1 |
| 20 | Классификация методов защиты информации | ОПК-6.У.1 |
| 21 | Понятие и классификация средств защиты информации | ОПК-6.У.1 |
| 22 | Назначение программных, криптографических и технических средств защиты | ОПК-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 |
|---|---|---|
| 1 | К правовым методам, обеспечивающим информационную безопасность, относятся:<br>1) Разработка аппаратных средств обеспечения правовых данных<br>2) Разработка и установка во всех компьютерных правовых сетях журналов учета действий | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 2 | Основными источниками угроз информационной безопасности являются все указанное в списке:<br>1) Хищение жестких дисков, подключение к сети, инсайдерство<br>2) Перехват данных, хищение данных, изменение архитектуры системы - Хищение данных, подкуп системных администраторов, нарушение регламента работы | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 3 | Виды информационной безопасности:<br>1) Персональная, корпоративная, государственная<br>2) Клиентская, серверная, сетевая<br>3) Локальная, глобальная, смешанная | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 4 | Основные объекты информационной безопасности:<br>1) Компьютерные сети, базы данных<br>2) Информационные системы, психологическое состояние пользователей<br>3) Бизнес-ориентированные, коммерческие системы | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 5 | Основными рисками информационной безопасности являются:<br>1) Искажение, уменьшение объема, перекодировка информации<br>2) Техническое вмешательство, выведение из строя оборудования сети<br>3) Потеря, искажение, утечка информации | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |

| | | |
|---|---|---|
| 6 | К основным принципам обеспечения информационной безопасности относится:<br>1) Экономической эффективности системы безопасности<br>2) Многоплатформенной реализации системы<br>3) Усиления защищенности всех звеньев системы | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 7 | Основными субъектами информационной безопасности являются:<br>1) руководители, менеджеры, администраторы компаний<br>2) органы права, государства, бизнеса<br>3) сетевые базы данных, фаерволлы | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 8 | К основным функциям системы безопасности можно отнести все перечисленное:<br>1) Установление регламента, аудит системы, выявление рисков<br>2) Установка новых офисных приложений, смена хостинг-компании<br>3) Внедрение аутентификации, проверки контактных данных пользователей | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 9 | Принципом информационной безопасности является принцип недопущения:<br>1) Неоправданных ограничений при работе в сети (системе)<br>2) Рисков безопасности сети, системы<br>3) Презумпции секретности | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 10 | Принципом политики информационной безопасности является принцип:<br>1) Невозможности миновать защитные средства сети (системы)<br>2) Усиления основного звена сети, системы<br>3) Полного блокирования доступа при риск-ситуациях | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 11 | Принципом политики информационной безопасности является принцип:<br>1) Усиления защищенности самого незащищенного звена сети (системы)<br>2) Перехода в безопасное состояние работы сети, системы<br>3) Полного доступа пользователей ко всем ресурсам сети, системы | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 12 | Принципом политики информационной безопасности является принцип:<br>1) Разделения доступа (обязанностей, привилегий) клиентам сети (системы)<br>2) Одноуровневой защиты сети, системы<br>3) Совместимых, однотипных программно-технических средств сети, системы | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 13 | К основным типам средств воздействия на компьютерную сеть относится:<br>1) Компьютерный сбой<br>2) Логические закладки («мины»)<br>3) Аварийное отключение питания | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 14 | Когда получен спам по e-mail с приложенным файлом, следует:<br>1) Прочитать приложение, если оно не содержит ничего ценного – удалить<br>2) Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама<br>3) Удалить письмо с приложением, не раскрывая (не читая) его | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 15 | Принцип Кирхгофа:<br>1) Секретность ключа определена секретностью открытого сообщения<br>2) Секретность информации определена скоростью передачи данных<br>3) Секретность закрытого сообщения определяется секретностью ключа | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 16 | ЭЦП – это:<br>1) Электронно-цифровой преобразователь | ОПК-2.З.1<br>ОПК-2.У.1 |

| | | |
|---|---|---|
| | 2) Электронно-цифровая подпись<br>3) Электронно-цифровой процессор | ОПК-2.В.1<br>ОПК-6.У.1 |
| 17 | Наиболее распространены угрозы информационной безопасности корпоративной системы:<br>1) Покупка нелицензионного ПО<br>2) Ошибки эксплуатации и неумышленного изменения режима работы системы<br>3) Сознательного внедрения сетевых вирусов | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 18 | Наиболее распространены угрозы информационной безопасности сети:<br>1) Распределенный доступ клиент, отказ оборудования<br>2) Моральный износ сети, инсайдерство<br>3) Сбой (отказ) оборудования, нелегальное копирование данных | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 19 | Наиболее распространены средства воздействия на сеть офиса:<br>1) Слабый трафик, информационный обман, вирусы в интернет<br>2) Вирусы в сети, логические мины (закладки), информационный перехват<br>3) Компьютерные сбои, изменение администрирования, топологии | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 20 | Утечкой информации в системе называется ситуация, характеризуемая:<br>1) Потерей данных в системе<br>2) Изменением формы информации<br>3) Изменением содержания информации | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 21 | Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:<br>1) Целостность<br>2) Доступность<br>3) Актуальность | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 22 | Угроза информационной системе (компьютерной сети) – это:<br>1) Вероятное событие<br>2) Детерминированное (всегда определенное) событие<br>3) Событие, происходящее периодически | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 23 | Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:<br>1) Регламентированной<br>2) Правовой<br>3) Защищаемой | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 24 | Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:<br>1) Программные, технические, организационные, технологические<br>2) Серверные, клиентские, спутниковые, наземные<br>3) Личные, корпоративные, социальные, национальные | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 25 | Окончательно, ответственность за защищенность данных в компьютерной сети несет:<br>1) Владелец сети<br>2) Администратор сети<br>3) Пользователь сети | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 26 | Политика безопасности в системе (сети) – это комплекс:<br>1) Руководств, требований обеспечения необходимого уровня безопасности<br>2) Инструкций, алгоритмов поведения пользователя в сети<br>3) Нормы информационного права, соблюдаемые в сети 28) | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |
| 27 | Наиболее важным при реализации защитных мер политики безопасности является:<br>1) Аудит, анализ затрат на проведение защитных мер<br>2) Аудит, анализ безопасности<br>3) Аудит, анализ уязвимостей, риск-ситуаций | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |

| | | |
|---|---|---|
| 28 | Цели информационной безопасности – своевременное обнаружение, предупреждение:<br>1) несанкционированного доступа, воздействия в сети<br>2) инсайдерства в организации<br>3) чрезвычайных ситуаций | ОПК-2.З.1<br>ОПК-2.У.1<br>ОПК-2.В.1<br>ОПК-6.У.1 |

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.

Выделяются следующие виды лекций:

- Вводная лекция

Вводная лекция к дисциплине знакомит обучающихся с целью и назначением курса, его ролью и местом в системе дисциплин. В ходе такой лекции связывается теоретический и практический материал с практикой бедующей работы, рассказывается общая методика работы над курсом, предлагаются литературные источники, помогающие усвоению материала дисциплины и освоению компетенций, ставятся научные проблемы,

выдвигаются гипотезы, определяется форма текущего контроля и промежуточной аттестации.

Вводная лекция к разделу. Аналогично вводной лекции к дисциплине раскрывает ряд вопросов, но связанных не с дисциплиной в целом, а с тематикой конкретного раздела.

- Обзорная лекция

Проводится с целью систематизации знаний на более высоком уровне, рассмотрения особо трудных вопросов дисциплины.

- Проблемная лекция

На данной лекции новое знание вводится как неизвестное, которое необходимо "открыть". В рамках лекции создается проблемная ситуация, которую обучающие решают поэтапно с подсказками и помощью преподавателя.

- Лекция вдвоем

Эта разновидность лекции является продолжением и развитием проблемного изложения материала в диалоге двух преподавателей. Здесь моделируются реальные ситуации обсуждения теоретических и практических вопросов двумя специалистами.

- Лекция с заранее запланированными ошибками

Данная лекция призвана активизировать внимание студентов, развивать их мыслительную деятельность, формировать умение выступать в роли экспертов.

Задача преподавателя состоит в том, чтобы заложить в лекцию определенное количество ошибок содержательного, методического, поведенческого характера. Подбираются наиболее типичные ошибки, которые обычно не выпячиваются, а как бы затушевываются. Задача студентов состоит в том, чтобы по ходу лекции отмечать ошибки, фиксировать и называть их в конце.

- Лекция-пресс-конференция

Преподаватель просит студентов задавать письменно вопросы по данной теме. В течение двух-трех минут студенты формулируют наиболее интересующие их вопросы и передают преподавателю, который в течение трех-пяти минут сортирует вопросы по их содержанию и начинает лекцию. Лекция излагается не как ответы на вопросы, а как связный текст, в процессе изложения которого формируются ответы.

- Лекция-консультация

Материал излагается в виде вопросов и ответов или вопросов, ответов и дискуссий.

Структура предоставления лекционного материала:

- Вводная часть лекции

Первое представление о лекции содержится уже в формулировке темы. Она должна быть краткой, выражать суть основной идеи, быть привлекательной по форме. Целесообразно здесь сказать на значение этой темы для последующего усвоения знаний и развития личности студентов, для будущей профессиональной деятельности. Далее можно сообщить цели лекции и ее план. Желательно сориентировать слушателей на последующий контроль знаний, полезно указать на связь нового материала с пройденным и предыдущим. Темп изложения этой части лекции, как правило, должен быть выше темпа изложения основного, что заставляет студентов психологически собраться и сосредоточиться. Вводная часть лекции обычно занимает 5-7 минут.

- Основная часть лекции

Переходу к изложению первого вопроса, как правило, должна предшествовать пауза. В это время лектор может проверить, все ли слушатели готовы к восприятию лекции (позы, выражения лиц, разговоры). Заметив студентов, не готовых к восприятию, опытные преподаватели произносят краткую мобилизующую фразу, останавливают взгляд на нерадивых, реже - называют фамилию, имя и не тратят время на длительные замечания.

Для того чтобы преодолеть потенциальную пассивность слушателей, необходимо всеми возможными способами придать лекции проблемный характер, побуждая слушателей к самостоятельной познавательной активности и творчеству.

К таким активным средствам можно отнести:

- обращение к студентам с вопросами, уточняющими понимание основных идей и фактов темы;
- организацию мини-столкновений различных точек зрения по выдвинутым преподавателем положениям;
- постановку вопросов, задач с множественностью решений и др.;
- индивидуальный стиль изложения материала;
- обеспечение обратной связи.

- Заключение

В процессе чтения лекции преподаватель должен позаботиться о ее завершении. Рассчитать время, а не прерывать лекцию на полуслове. Обычно для заключения материала бывает достаточно 5-7 минут. Завершая лекцию, преподаватель отвечает на вопросы слушателей, подводит итог, дает методические указания к самостоятельной работе, комментирует предлагаемую литературу. Заканчивать лекцию нужно конструктивно по содержанию и положительно по эмоциональному настрою. Студенты должны уйти заинтересованными, заинтригованными, желающими опробовать завтра же предложения лектора, а также в хорошем настроении и активном тонусе.

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.

Задания и требования к лабораторным работам размещены в Личном кабинете ГУАП в разделе дисциплины.

Структура и форма отчета о лабораторной работе.

Отчет о лабораторной работе сдается в электронном виде (документ Word, документ PDF) через Личный кабинет ГУАП. Отчет к лабораторной работе содержит следующие элементы:

– титульный лист с названием дисциплины, номером и названием лабораторной работы;
– цели и задачи работы;
– приборы и реактивы (при необходимости);
– задание;
– ход работы (при необходимости);
– контрольные примеры (при необходимости);
– выводы;

Требования к оформлению отчета о лабораторной работе.

– Общие требования и рекомендации по выполнению письменных работ : методические указания / С.-Петерб. гос. ун-т аэрокосм. приборостроения ; сост. А. А. Сорокин. - СПб. : Изд-во ГУАП, 2017. - 32 с.

– Общие требования и рекомендации по выполнению письменных работ : методические указания (с изменениями от 09.01.2019) [Электронный ресурс] / Ивангородский филиал С.-Петерб. гос. ун-т аэрокосм. приборостроения ; сост. А. А. Сорокин. - Ивангород : 2019. - 37 с. URL: http://ifguap.ru/rp/ReportsFormattingRules.pdf, Личный кабинет ГУАП

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 обучающихсяявляются:

– учебно-методический материал по дисциплине;.

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.

Возможные методы текущего контроля:

– устный опрос на занятиях;
– систематическая проверка выполнения индивидуальных и домашних заданий;
– защита отчетов по лабораторным работам;
– проведение контрольных работ;
– тестирование;
– контроль самостоятельных работ;
– проведение контрольных работ;
– доклад на научной конференции;
– написание научной статьи.

11.5. Методические указания для обучающихся по прохождению тестирования

Использование тестовых заданий возможно как при текущем контроле, так и при проведении промежуточной аттестации. Тесты могут проводиться как в письменной форме, так и с использованием электронных средств обучения.

Можно выделить основные уровни теста, в которых проверка возрастает от контроля знаний (индикатор достижения компетенции - "знать") до применения навыков при решении типовых и нетиповых задач ((индикаторы достижения компетенции - "уметь" и "владеть"):

– Первый уровень - узнавание ранее изученного материала;

– Второй уровень - репродуктивный - в заданиях не содержится материала для ответа или же его извлечение требует не только запоминания материала, но и его понимания (подстановка, конструктивный тест, типовая задача);

– Третий уровень - нетиповые задачи повышенной сложности, для которых требуется самостоятельное нахождение методов решения;

– Смешанный - использование элементов всех трех уровней для проверки разных индикаторов достижения компетенций.

Критерии оценки тестовых работ базируются на 100-бальной шкале согласно МДО ГУАП. СМК 2.77 "Положение о модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП" (допустимо применение любого количественного показателя оценки с приведением его к 100-процентной шкале):

– менее 55 - "не зачтено" или "неудовлетворительно" (2);

– от 55 до 69 - "зачтено" или "удовлетворительно" (3);

– от 70 до 84 - "зачтено" или "хорошо" (4);

– от 85 до 100 - "зачтено" или "отлично" (5).

11.6. Методические указания для обучающихся по прохождению промежуточной аттестации.

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

– 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».

Дифференцированный зачет проводится в одной из следующих форм:

– в письменной форме в виде теста

В случае дистанционной формы промежуточной аттестации, дифференцированный зачет проводится в виде теста с применением средств электронного обучения.

Выполнение обучающимся лабораторных работ не в полном объеме может привести к понижению оценки за дисциплину из-за низкого уровня освоения компетенций:

– выполнение менее 75% лабораторных работ - понижение максимальной оценки на 1 балл;

– выполнение менее 50% лабораторных работ - понижение максимальной оценки на 2 балла;

– невыполнение лабораторных работ - понижение максимальной оценки на 3 балла.

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