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

Кафедра № 33

УТВЕРЖДАЮ
Руководитель образовательной программы

доц.,к.культурол.,доц.
(должность, уч. степень, звание)

Н.В. Выжлецова
(инициалы, фамилия)

(подпись)

«25» февраля 2026 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы информационной безопасности»
(Наименование дисциплины)

| | |
|---|---|
| Код направления подготовки/ специальности | 51.03.01 |
| Наименование направления подготовки/ специальности | Культурология |
| Наименование направленности/ специализации | Цифровые проекты в креативных индустриях |
| Форма обучения | очная |
| Год приема | 2026 |

Санкт-Петербург– 2026

Лист согласования рабочей программы дисциплины

Программу составил (а)

| доц., к.э.н., доц. | 20.02.26 | Т.Н. Елина |
|---|---|---|
| (должность, уч. степень, звание) | (подпись, дата) | (инициалы, фамилия) |

Программа одобрена на заседании кафедры № 33
«20» февраля 2026 г, протокол № 7

Заведующий кафедрой № 33

| д.т.н.,проф. | 20.02.26 | С.В. Беззатеев |
|---|---|---|
| (уч. степень, звание) | (подпись, дата) | (инициалы, фамилия) |

Заместитель декана факультета №6 по методической работе

| | 24.02.2026 | М.Б. Капелюш |
|---|---|---|
| (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 51.03.01 «Культурология» направленности/специализации «Цифровые проекты в креативных индустриях». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

УК-1 «Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач»

УК-2 «Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений»

УК-6 «Способен управлять своим временем, выстраивать и реализовывать траекторию саморазвития на основе принципов образования в течение всей жизни»

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 зачета (3 семестр).

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов.

Язык обучения по дисциплине «русский »

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Дисциплина имеет своей целью: обеспечить выполнение требований, изложенных в федеральном государственном образовательном стандарте высшего профессионального образования. Изучение дисциплины направлено на формирование перечисленных ниже элементов универсальных и общепрофессиональных 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 |
|---|---|---|
| Универсальные компетенции | УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач | УК-1.З.1 знать методики поиска, сбора и обработки информации, в том числе с использованием информационных технологий, включая интеллектуальные<br>УК-1.В.1 владеть навыками критического анализа и синтеза информации, в том числе с помощью цифровых инструментов |
| Универсальные компетенции | УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений | УК-2.З.1 знать виды ресурсов и ограничения для решения поставленных задач<br>УК-2.У.3 уметь выдвигать альтернативные варианты действий с целью выбора оптимальных способов решения задач, в том числе с помощью цифровых средств<br>УК-2.В.3 владеть навыками использования цифровых средств для решения поставленной задачи |
| Универсальные компетенции | УК-6 Способен управлять своим временем, выстраивать и реализовывать траекторию | УК-6.В.2 владеть навыками использования цифровых инструментов для саморазвития и самообразования |

| | | |
|---|---|---|
| | саморазвития на основе принципов образования в течение всей жизни | |
| Общепрофессиональные компетенции | ОПК-2 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности | ОПК-2.З.1 знать основные возможности, предоставляемые современными информационно-коммуникационными технологиями, в том числе интеллектуальными для решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности<br>ОПК-2.У.1 уметь применять информационно-коммуникационные технологии, в том числе интеллектуальные с учетом основных требований информационной безопасности в соответствии с поставленными задачами<br>ОПК-2.В.1 владеть навыками решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий, в том числе интеллектуальных с учетом основных требований информационной безопасности |

## 2. Место дисциплины в структуре ОП

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

- «Информатика»,
- «Информационные технологии»

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

- «Теория интернета»,
- «Большие данные»

## 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 |
|---|---|---|
| | | №3 |
| 1 | 2 | 3 |
| ***Общая трудоемкость дисциплины***, ЗЕ/ (час) | 3/ 108 | 3/ 108 |
| ***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) | 57 | 57 |
| ***Вид промежуточной аттестации*:** зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.) | Зачет, | Зачет, |

## 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/КР (час) | СР (час) |
|---|---|---|---|---|---|
| Семестр 3 | | | | | |
| Раздел 1. Введение в курс «Основы информационной безопасности» | 2 | | | | 4 |
| Раздел 2. Сущность и понятие информационной безопасности | 2 | | | | 5 |
| Раздел 3. Значение информационной безопасности и ее место в системе национальной безопасности | 4 | | 4 | | 8 |
| Раздел 4. Сущность и понятие защиты информации | 4 | | 4 | | 8 |
| Раздел 5. Состав и классификация носителей защищаемой информации | 4 | | 4 | | 8 |
| Раздел 6. Понятие и структура угроз защищаемой информации | 4 | | 5 | | 8 |
| Раздел 7. Объекты защиты информации | 6 | | | | 8 |
| Раздел 8. Классификация видов, методов и средств защиты информации | 8 | | | | 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 | Раздел 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. Анализ нормативных источников, научной и учебной литературы. Знания и умения студентов, которые должны быть получены в результате изучения курса. |
| 2 | Раздел 2. Сущность и понятие информационной безопасности<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". |
| 3 | Раздел 3. 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.<br>Понятие и современная концепция национальной безопасности. Место информационной, безопасности, в системе национальной безопасности. |
| 4 | Раздел 4. 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". |
| 5 | Раздел 5. 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. |
| 6 | Раздел 6. 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. |
| 7 | Раздел 7. 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. |
| 8 | Раздел 8. 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 | | | | | |
| | | | | | |
| 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 3 | | | | |
| 1. | Исследование уязвимости информации | 4 | | 3 |
| 2. | Исследование видов уязвимости | 4 | | 4 |
| 3. | Исследование форм уязвимости | 4 | | 5 |
| 4. | Построение алгоритмов социальной инженерии и способы защиты от них | 5 | | 6 |
| Всего | | 17 | | |

4.5. Выполнение курсового проекта/ 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 3, 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) | 16 | 16 |
| Домашнее задание (ДЗ) | | |
| Контрольные работы заочников (КРЗ) | | |
| Подготовка к промежуточной аттестации (ПА) | 11 | 11 |
| 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. разделов 6-11.

## 6. Перечень печатных и электронных учебных изданий

Перечень печатных и электронных учебных изданий приведен в таблице 8.

Таблица 8– Перечень печатных и электронных учебных изданий

| Шифр/ URL адрес | Библиографическая ссылка | Количество экземпляров в библиотеке (кроме электронных экземпляров) |
|---|---|---|
| 004 С 24 | Свинарчук, Андрей Александрович (канд. техн. наук). Основы информационной безопасности : учебно-методическое пособие / А. А. Свинарчук ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2023. - 94 с. : рис., табл. - Библиогр.: с. 90 (12 назв.). - Б. ц. - Текст : непосредственный | 5 |
| 004.05 В 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. Информационная безопасность [Текст]: научно-популярная литература / В. Ф. Шаньгин. - М.: ДМК Пресс, 2014. - 702 с | 5 |
| Х Я 47 | Яковец, Е. Н. Правовые основы обеспечения информационной безопасности Российской Федерации [Текст] : учебное пособие / Е. Н. Яковец. - М. : Юрлитинформ, 2010. - 336 с. | 5 |

| | | |
|---|---|---|
| | http://e.lanbook.com/books/element.php?pl1_id=3032 Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : ДМК Пресс, 2012. — 592 с | |
| 004 М 48 | Мельников, В. П. Защита информации [Текст] : учебник / В. П. Мельников, А. И. Куприянов, А. Г. Схиртладзе ; ред. В. П. Мельников. - М. : Академия, 2014. - 304 с. | 5 |
| 004 Р 98 | Рябко, Б. Я. Криптографические методы защиты информации [Текст] : учебное пособие / Б. Я. Рябко, А. Н. Фионов. - 2-е изд., стер. - М. : Горячая линия - Телеком, 2014. - 229 с. | 10 |
| | http://e.lanbook.com/books/element.php?pl1_id=4959 Титов, А.А. Инженерно-техническая защита информации [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : ТУСУР (Томский государственный университет систем управления и радиоэлектроники), 2010. — 195 с. | |

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

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

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

| URL адрес | Наименование |
|---|---|
| | Не предусмотрено |

## 8. Перечень информационных технологий

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

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

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

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

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

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

## 9. Материально-техническая база

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

Таблица 12 – Состав материально-технической базы

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

10. Оценочные средства для проведения промежуточной аттестации

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

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

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

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

Таблица 14 –Критерии оценки уровня сформированности компетенций

| Оценка компетенции<br>5-балльная шкала | Характеристика сформированных компетенций |
|---|---|
| «отлично»<br>«зачтено» | Обучающийся:<br>– глубоко и всесторонне усвоил программный материал;<br>– уверенно, логично, последовательно и грамотно его излагает;<br>– опираясь на знания основной и дополнительной литературы, тесно связывает 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.<br>– правильно выполнил от 90% до 100% тестовых заданий**. |
| «хорошо»<br>«зачтено» | Обучающийся:<br>– 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;<br>– владеет системой специализированных понятий.<br>– правильно выполнил от 70% до 89% тестовых заданий**. |
| «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 |

| Оценка компетенции<br>5-балльная шкала | Характеристика сформированных компетенций |
|---|---|
| | направления;<br>– слабо аргументирует научные положения;<br>– затрудняется в формулировании выводов и обобщений;<br>– частично владеет системой специализированных понятий.<br>– правильно выполнил от 51% до 69% тестовых заданий**. |
| «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.<br>– правильно выполнил менее 51% тестовых заданий**. |

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 | Понятие информационной безопасности (ИБ) и основные термины (защита, угроза, уязвимость).<br>Триада CIA (Confidentiality, Integrity, Availability): конфиденциальность, целостность, доступность — понятие и примеры нарушений.<br>Предпосылки и цели обеспечения информационной безопасности.<br>Виды информационной безопасности: персональная, корпоративная, государственная.<br>Объекты и субъекты защиты информации. | УК-1.З.1 |
| 2 | Доктрина информационной безопасности Российской Федерации (основные положения).<br>Информационная безопасность человека и общества.<br>Компьютерные преступления: определение, классификация и основные технологии совершения.<br>Современная концепция обеспечения ИБ.<br>Роль человеческого фактора в обеспечении информационной безопасности.<br>Классификация угроз информационной безопасности (источники, цели, виды воздействия).<br>Основные каналы утечки информации.<br>Технические каналы утечки информации: понятие и способы защиты.<br>Виды сетевых атак: DoS, DDoS, Man-in-the-Middle (MITM). | УК-1.В.1 |
| 3 | Социальная инженерия: методы и способы | УК-2.З.1 |

| | | |
|---|---|---|
| | противодействия.<br>Вредоносное программное обеспечение: вирусы, черви, трояны, Ransomware.<br>Угрозы безопасности персональных данных.<br>Угрозы коммерческой тайны и инсайдерство.<br>Методы оценки рисков информационной безопасности.<br>Что такое уязвимость (vulnerability) и чем она отличается от угрозы?<br>Политика безопасности информационной системы: назначение и структура.<br>Методы аутентификации и идентификации пользователей.<br>Виды аутентификации (однофакторная, двухфакторная, многофакторная).<br>Дискреционная и мандатная модели управления доступом. | |
| 4 | Механизмы защиты: технические, правовые, организационные.<br>Криптографические методы защиты информации (симметричные и асимметричные).<br>Хеширование: понятие и использование для проверки целостности.<br>Межсетевые экраны (Firewalls): функции, типы (пакетные, уровня приложений). | УК-2.У.3 |
| 5 | Системы обнаружения и предотвращения вторжений (IDS/IPS).<br>Антивирусная защита: принципы работы.<br>VPN (виртуальные частные сети) — назначение и виды.<br>Резервное копирование (Backup) как средство обеспечения доступности данных.<br>Безопасность беспроводных сетей (Wi-Fi).<br>Защита мобильных устройств.<br>Защита информации в облачных вычислениях | УК-2.В.3 |
| 6 | Правовые методы обеспечения информационной безопасности.<br>Законодательство РФ в области защиты информации (ФЗ-152, ФЗ-149).<br>Государственная и коммерческая тайна: понятие и защита.<br>Персональные данные: классификация и правовой режим защиты.<br>Стандарты в области информационной безопасности (ГОСТ Р ИСО/МЭК 27001). | УК-6.В.2 |
| 7 | Система защиты информации организации: структура и принципы создания.<br>Оценка рисков: определение, этапы. | ОПК-2.З.1 |
| 8 | Бизнес-непрерывность и восстановление после инцидентов (BCP/DRP).<br>Обучение персонала основам кибербезопасности.<br>Аудит безопасности информационной системы. | ОПК-2.У.1 |
| 9 | Принципы работы IPsec.<br>Методы защиты от сниффинга пакетов.<br>Методы устранения угрозы IP-спуфинга.<br>Атаки на уровне приложений (SQL-инъекции, XSS).<br>Фишинг: определение, виды (smishing, vishing) и признаки. | ОПК-2.В.1 |

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

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

| № п/п | Примерный перечень тем для выполнения курсового проекта/ 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 | 1) К правовым методам, обеспечивающим информационную безопасность, относятся:<br>- Разработка аппаратных средств обеспечения правовых данных<br>- Разработка и установка во всех компьютерных правовых сетях журналов учета действий<br>+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности<br>2) Основными источниками угроз информационной безопасности являются все указанное в списке:<br>- Хищение жестких дисков, подключение к сети, инсайдерство<br>+ Перехват данных, хищение данных, изменение архитектуры системы<br>- Хищение данных, подкуп системных администраторов, нарушение регламента работы<br>3) Виды информационной безопасности:<br>+ Персональная, корпоративная, государственная<br>- Клиентская, серверная, сетевая<br>- Локальная, глобальная, смешанная<br>4) Цели информационной безопасности – своевременное обнаружение, предупреждение:<br>+ несанкционированного доступа, воздействия в сети<br>- инсайдерства в организации<br>- чрезвычайных ситуаций<br>5) Основные объекты информационной безопасности:<br>+ Компьютерные сети, базы данных<br>- Информационные системы, психологическое состояние пользователей<br>- Бизнес-ориентированные, коммерческие системы | УК-1.З.1 |
| 2 | 6) Основными рисками информационной безопасности являются:<br>- Искажение, уменьшение объема, перекодировка информации<br>- Техническое вмешательство, выведение из строя оборудования сети<br>+ Потеря, искажение, утечка информации<br>7) К основным принципам обеспечения информационной безопасности относится:<br>+ Экономической эффективности системы безопасности<br>- Многоплатформенной реализации системы<br>- Усиления защищенности всех звеньев системы | УК-1.В.1 |

| | | |
|---|---|---|
| | 8) Основными субъектами информационной безопасности являются:<br>- руководители, менеджеры, администраторы компаний<br>+ органы права, государства, бизнеса<br>- сетевые базы данных, фаерволлы<br>9) К основным функциям системы безопасности можно отнести все перечисленное:<br>+ Установление регламента, аудит системы, выявление рисков<br>- Установка новых офисных приложений, смена хостинг-компании<br>- Внедрение аутентификации, проверки контактных данных пользователей<br>тест<br>10) Принципом информационной безопасности является принцип недопущения:<br>+ Неоправданных ограничений при работе в сети (системе)<br>- Рисков безопасности сети, системы<br>- Презумпции секретности | |
| 3 | 11) Принципом политики информационной безопасности является принцип:<br>+ Невозможности миновать защитные средства сети (системы)<br>- Усиления основного звена сети, системы<br>- Полного блокирования доступа при риск-ситуациях<br>12) Принципом политики информационной безопасности является принцип:<br>+ Усиления защищенности самого незащищенного звена сети (системы)<br>- Перехода в безопасное состояние работы сети, системы<br>- Полного доступа пользователей ко всем ресурсам сети, системы<br>13) Принципом политики информационной безопасности является принцип:<br>+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)<br>- Одноуровневой защиты сети, системы<br>- Совместимых, однотипных программно-технических средств сети, системы<br>14) К основным типам средств воздействия на компьютерную сеть относится:<br>- Компьютерный сбой<br>+ Логические закладки («мины»)<br>- Аварийное отключение питания<br>15) Когда получен спам по e-mail с приложенным файлом, следует:<br>- Прочитать приложение, если оно не содержит ничего ценного – удалить<br>- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама<br>+ Удалить письмо с приложением, не раскрывая (не читая) его | УК-2.З.1 |
| 4 | 16) Принцип Кирхгофа:<br>- Секретность ключа определена секретностью открытого сообщения<br>- Секретность информации определена скоростью передачи данных<br>+ Секретность закрытого сообщения определяется секретностью ключа | УК-2.У.3 |

| | | |
|---|---|---|
| | 17) ЭЦП – это:<br>- Электронно-цифровой преобразователь<br>+ Электронно-цифровая подпись<br>- Электронно-цифровой процессор<br>18) Наиболее распространены угрозы информационной безопасности корпоративной системы:<br>- Покупка нелицензионного ПО<br>+ Ошибки эксплуатации и неумышленного изменения режима работы системы<br>- Сознательного внедрения сетевых вирусов<br>19) Наиболее распространены угрозы информационной безопасности сети:<br>- Распределенный доступ клиент, отказ оборудования<br>- Моральный износ сети, инсайдерство<br>+ Сбой (отказ) оборудования, нелегальное копирование данных<br>20) Наиболее распространены средства воздействия на сеть офиса:<br>- Слабый трафик, информационный обман, вирусы в интернет<br>+ Вирусы в сети, логические мины (закладки), информационный перехват<br>- Компьютерные сбои, изменение администрирования, топологии | |
| 5 | 21) Утечкой информации в системе называется ситуация, характеризуемая:<br>+ Потерей данных в системе<br>- Изменением формы информации<br>- Изменением содержания информации<br>22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:<br>+ Целостность<br>- Доступность<br>- Актуальностьl<br>23) Угроза информационной системе (компьютерной сети) – это:<br>+ Вероятное событие<br>- Детерминированное (всегда определенное) событие<br>- Событие, происходящее периодически<br>24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:<br>- Регламентированной<br>- Правовой<br>+ Защищаемой<br>25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:<br>+ Программные, технические, организационные, технологические<br>- Серверные, клиентские, спутниковые, наземные<br>- Личные, корпоративные, социальные, национальные | УК-2.В.3 |
| 6 | 26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:<br>+ Владелец сети<br>- Администратор сети<br>- Пользователь сети<br>27) Политика безопасности в системе (сети) – это комплекс:<br>+ Руководств, требований обеспечения необходимого уровня безопасности | УК-6.В.2 |

| | | |
|---|---|---|
| | - 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<br>29) Кто является основным ответственным за определение уровня классификации информации?<br>-Руководитель среднего звена<br>-Высшее руководство<br>+Владелец<br>-Пользователь<br>30) Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?<br>+Сотрудники<br>-Хакеры<br>-Атакующие<br>-Контрагенты (лица, работающие по договору) | |
| 7 | 31) Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?<br>-Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования<br>-Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации<br>+Улучшить контроль за безопасностью этой информации<br>-Снизить уровень классификации этой информации<br>32) Что самое главное должно продумать руководство при классификации данных?<br>Варианты ответа:<br>-Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным<br>+Необходимый уровень доступности, целостности и конфиденциальности<br>-Оценить уровень риска и отменить контрмеры<br>-Управление доступом, которое должно защищать данные<br>33) Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?<br>-Владельцы данных<br>-Пользователи<br>-Администраторы<br>+Руководство<br>34) Что такое процедура?<br>-Правила использования программного и аппаратного обеспечения в компании<br>+Пошаговая инструкция по выполнению задачи<br>-Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах<br>-Обязательные действия<br>35) Какой фактор наиболее важен для того, чтобы быть уверенным | ОПК-2.3.1 |

| | | |
|---|---|---|
| | в успешном обеспечении безопасности в компании?<br>+Поддержка высшего руководства<br>-Эффективные защитные меры и методы их внедрения<br>-Актуальные и адекватные политики и процедуры безопасности<br>-Проведение тренингов по безопасности для всех сотрудников | |
| 8 | 36) Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?<br>-Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски<br>-Когда риски не могут быть приняты во внимание по политическим соображениям<br>-Когда необходимые защитные меры слишком сложны<br>+Когда стоимость контрмер превышает ценность актива и потенциальные потери<br>37) Что такое политики безопасности?<br>-Пошаговые инструкции по выполнению задач безопасности<br>-Общие руководящие требования по достижению определенного уровня безопасности<br>+Широкие, высокоуровневые заявления руководства<br>-Детализированные документы по обработке инцидентов безопасности<br><br>39) Какая из приведенных техник является самой важной при выборе конкретных защитных мер?<br>-Анализ рисков<br>+Анализ затрат / выгоды<br>-Результаты ALE<br>-Выявление уязвимостей и угроз, являющихся причиной риска<br>40) Что лучше всего описывает цель расчета ALE?<br>-Количественно оценить уровень безопасности среды<br>-Оценить возможные потери для каждой контрмеры<br>-Количественно оценить затраты / выгоды<br>+Оценить потенциальные потери от угрозы в год | ОПК-2.У.1 |
| 9 | 41) Тактическое планирование – это:<br>+Среднесрочное планирование<br>-Долгосрочное планирование<br>-Ежедневное планирование<br>-Планирование на 6 месяцев<br>42) Что является определением воздействия (exposure) на безопасность?<br>+Нечто, приводящее к ущербу от угрозы<br>-Любая потенциальная опасность для информации или систем<br>-Любой недостаток или отсутствие информационной безопасности<br>-Потенциальные потери от угрозы<br>43) Эффективная программа безопасности требует сбалансированного применения:<br>+Технических и нетехнических методов<br>-Контрмер и защитных механизмов<br>-Физической безопасности и технических средств защиты<br>-Процедур безопасности и шифрования<br>44) Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют: | ОПК-2.В.1 |

| | | |
|---|---|---|
| | -Внедрение управления механизмами безопасности<br>-Классификацию данных после внедрения механизмов безопасности<br>+Уровень доверия, обеспечиваемый механизмом безопасности<br>-Соотношение затрат / выгод<br>45) Как рассчитать остаточный риск?<br>Варианты ответа:<br>-Угрозы х Риски х Ценность актива<br>-(Угрозы х Ценность актива х Уязвимости) х Риски<br>-SLE х Частоту = ALE<br>+(Угрозы х Уязвимости х Ценность актива) х Недостаток контроля | |

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.

Методические указания по освоению лекционного материала имеются в изданном виде в библиотеке ГУАП Свинарчук, Андрей Александрович (канд. техн. наук). Основы информационной безопасности : учебно-методическое пособие / А. А. Свинарчук ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2023. - 94 с. : рис., табл. - Библиогр.: с. 90 (12 назв.). - Б. ц. - Текст : непосредственный

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.

В процессе выполнения самостоятельной работы у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет ему 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;

– методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

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

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

Для успешного прохождения текущего контроля необходимо выполнить лабораторные работы, загрузить их в личный кабинет и пройти процедуру защиты каждой работы. Оценки за работы выставляются по пятибалльной шкале.

11.5. Методические указания для обучающихся по прохождению промежуточной аттестации.

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

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

Для положительной оценки необходимо каждую лабораторную работу защитить на оценку не ниже удовлетворительно.

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