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

Кафедра № 23

УТВЕРЖДАЮ
Руководитель образовательной программы

Старший преподаватель
(должность, уч. степень, звание)

Е.П. Виноградова
(инициалы, фамилия)

(подпись)

«17» февраля 2025 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы информационной безопасности»
(Наименование дисциплины)

Код направления подготовки/ специальности	11.03.04
Наименование направления подготовки/ специальности	Электроника и наноэлектроника
Наименование направленности	Промышленная электроника
Форма обучения	очная
Год приема	2025

Санкт-Петербург– 2025

Лист согласования рабочей программы дисциплины

Программу составил (а)

ст.преподаватель, к.т.н. (должность, уч. степень, звание) — 17.02.25 (подпись, дата) — В.К. Лосев (инициалы, фамилия)

Программа одобрена на заседании кафедры № 23
«17» февраля 2025 г, протокол № 6/25

Заведующий кафедрой № 23

д.т.н.,проф. (уч. степень, звание) — 17.02.25 (подпись, дата) — А.Р. Бестугин (инициалы, фамилия)

Заместитель директора института №2 по методической работе

доц.,к.т.н.,доц. (должность, уч. степень, звание) — 17.02.25 (подпись, дата) — Н.В. Марковская (инициалы, фамилия)

Аннотация

Дисциплина «Основы информационной безопасности» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 11.03.04 «Электроника и наноэлектроника» направленности «Промышленная электроника». Дисциплина реализуется кафедрой «№23».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

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»

ОПК-3 «Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной безопасности»

ПК-6 «Способен использовать стандартные программные средства компьютерного моделирования приборов, схем, устройств и установок электроники и наноэлектроники различного функционального назначения»

Содержание дисциплины охватывает круг вопросов, связанных с сущностью и значением 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 обучающегося.

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

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 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
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.В.1 владеть навыками выбора оптимального способа решения задач с учетом действующих правовых норм
Общепрофессиональные компетенции	ОПК-3 Способен применять методы поиска, хранения, обработки, анализа и представления в требуемом формате информации из различных источников и баз данных, соблюдая при этом основные требования информационной	ОПК-3.3.1 знать, как использовать информационно-коммуникационные технологии при поиске необходимой информации ОПК-3.В.1 владеть навыками обеспечения информационной безопасности.

	безопасности	
Профессиональные компетенции	ПК-6 Способен использовать стандартные программные средства компьютерного моделирования приборов, схем, устройств и установок электроники и наноэлектроники различного функционального назначения	ПК-6.З.1 знать номенклатуру средств компьютерного моделирования электронных приборов и устройств, их функциональные возможности и ограничения. ПК-6.У.1 уметь выбирать средства компьютерного моделирования электронных приборов и устройств.

2. Место дисциплины в структуре ОП

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

– Информатика

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

3. Объем и трудоемкость дисциплины

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

Таблица 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№7
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	3/ 108	3/ 108
Из них часов практической подготовки	5	5
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.**)	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) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 7					
Раздел 1. Информация как объект защиты.	4		2		7
Раздел 2. Понятийный аппарат информационной безопасности.	4		2		7
Раздел 3. Государственная политика информационной безопасности.	4		2		7
Раздел 4. Угрозы безопасности информации.	4		2		7
Раздел 5. Меры противодействия угрозам безопасности.	4		2		7
Раздел 6. Криптографические методы защиты информации.	4		2		7
Раздел 7. Основные механизмы защиты от несанкционированного доступа.	4		2		7
Раздел 8. Информационная безопасность компьютерных сетей.	6		3		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. Информация как объект защиты. Понятие об информации. Уровни представления информации. Свойства защищаемой информации. Виды тайн. Правовой режим информационных ресурсов.
2	Раздел 2. Понятийный аппарат информационной безопасности. Виды, способы, замысел, объект, техника защиты информации. Виды нарушителя и классификация угроз. Банк данных угроз безопасности информации ФСТЭК России.
3	Раздел 3. Государственная политика информационной безопасности. Государственная система обеспечения информационной безопасности. Законодательная основа обеспечения информационной безопасности. Безопасность критической информационной инфраструктуры РФ. Доктрина информационной безопасности РФ. ФСТЭК.
4	Раздел 4. Угрозы безопасности информации. Несанкционированные операции с информацией. Перечень типовых угроз. Классификация уязвимостей и угроз. Классификация способов НСД. Типовые атаки на

	коммуникационные протоколы. Международные базы данных и реестры уязвимостей.
5	Раздел 5. Меры противодействия угрозам безопасности. Правовое обеспечение информационной безопасности. Организационные, физические, технические меры. Политика информационной безопасности организации.
6	Раздел 6. Криптографические методы защиты информации. Основные задачи криптографии. Криптографические системы. Криптографические протоколы. Цифровая подпись. Хеш-функция. Стандарты в области криптографической защиты информации.
7	Раздел 7. Основные механизмы защиты от несанкционированного доступа. Контроль целостности, идентификация, протоколирование и аудит. Управление доступом, защита от вредоносных программ. Защита межсетевого взаимодействия, защита информации при передаче, предотвращение утечек информации.
8	Раздел 8. Информационная безопасность компьютерных сетей. Угрозы корпоративной сети. Защита периметра. Основные механизмы защиты. Базовые средства защиты компьютерных сетей (межсетевые экраны, системы анализа защищенности, системы обнаружения атак и др.). Виртуальные частные сети (VPN). Аудит безопасности.

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	Построение модели угроз информационной системы	3		4
2	Построение модели утечки информационной безопасности	3		1
3	Построение алгоритмов социальной инженерии и способы защиты от них	3		7

4	Исследование уязвимости информации	2		5
5	Анализ обрабатываемой информации с точки зрения видов тайн и формирование требований к ее защите	3		2
6	Сравнение криптографических и технических средств защиты	3		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)	50	50
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	7	7
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)		
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/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
	Нестеров С.А. Основы информационной безопасности: учебное пособие. – Лань, 2019. – 324 с.	

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

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

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

URL адрес	Наименование
http://www.consultant.ru	Общероссийская Сеть КонсультантПлюс. Справочная правовая система.
http://www.intuit.ru/studies/courses/10/10/info	Основы информационной безопасности [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ".
http://www.intuit.ru/studies/courses/2259/155/info	Антивирусная защита компьютерных систем [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ".
http://www.intuit.ru/studies/courses/102/102/info	Безопасность сетей [Электронный ресурс] // Национальный Открытый Университет "ИНТУИТ".

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
Дифференцированный зачёт	Список вопросов; Тесты; 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 5-балльная шкала	Характеристика сформированных компетенций
«отлично» «зачтено»	– обучающийся глубоко и всесторонне усвоил программный материал; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно привязывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий.
«хорошо» «зачтено»	– обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; – не допускает существенных неточностей; – увязывает усвоенные знания с практической деятельностью направления; – аргументирует научные положения; – делает выводы и обобщения; – владеет системой специализированных понятий.
«удовлетворительно» «зачтено»	– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; – допускает несущественные ошибки и неточности; – испытывает затруднения в практическом применении знаний направления; – слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий.
«неудовлетворительно» «не зачтено»	– обучающийся не усвоил значительной части программного материала; – допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; – испытывает трудности в практическом применении знаний; – не может аргументировать научные положения;

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
	– 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	Роль информации в современном мире. Понятие о защищаемой информации	ПК-6.З.1
2	Теория информационной безопасности. Основные направления	ОПК-3.В.1
3	Обеспечение ИБ и направления защиты	
4	Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации	УК-2.В.1
5	Понятие о защищаемой информации. Свойства информации	ПК-6.З.1
6	Классификация и виды угроз информационной безопасности	ОПК-3.В.1
7	Угрозы нарушения конфиденциальности информации. Особенности и примеры реализации угроз	ОПК-3.З.1
8	Угрозы нарушения целостности информации. Особенности и примеры реализации угроз	ОПК-3.З.1
9	Угроза нарушения доступности информации. Особенности и примеры реализации угроз	ОПК-3.З.1
10	Идентификация и аутентификация. Использование парольной защиты. Недостатки парольной защиты	ПК-6.З.1
11	Понятие электронной подписи	
12	Организационные меры обеспечения информационной безопасности. Служба безопасности предприятия	УК-2.В.1
13	Организация внутри объектового режима предприятия. Организация охраны	УК-2.В.1
14	Криптографические меры обеспечения информационной безопасности. Классификация криптографических алгоритмов	ПК-6.З.1
15	Программно-аппаратные защиты информации. Межсетевые экраны, их функции и назначения	ПК-6.У.1
16	Программно-аппаратные защиты информации. Антивирусные средства, их функции и назначения	ПК-6.У.1
17	Понятие и классификация средств защиты информации.	ОПК-3.В.1

	Назначение программных, криптографических и технических средств защиты.	
18	Понятие носитель защищаемой информации. Соотношение между носителем и источником информации	ПК-6.У.1
19	Физический средства защиты информации. Защита от НСД	ОПК-3.В.1
20	Защита компьютерных сетей. Аудит информации	ОПК-3.З.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	*Инструкция. Прочитайте задание и выберите один правильный ответ.* Когда получен спам по e-mail с приложенным файлом, следует: 1. Прочитать приложение, если оно не содержит ничего ценного – удалить 2. Сохранить приложение в парке «Спам», затем выяснить IP-адрес генератора спама 3. Удалить письмо с приложением, не раскрывая (не читая) его	ОПК-3.В.1
2	Естественные угрозы безопасности информации вызваны: 1. Деятельностью человека 2. Воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека; 3. Корыстными устремлениями злоумышленников;	ПК-6.З.1
3	Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется: 1. Пассивный перехват 2. Аудиоперехват 3. Видеоперехват	ПК-6.У.1
4	Угроза информационной системе (компьютерной сети) – это: 1. Вероятное событие 2. Детерминированное (всегда определенное) событие 3. Событие, происходящее периодически)	УК-2.В.1
5	Потенциальная возможность неправомерного или случайного воздействия на объект защиты, приводящая к потере или разглашению информации: 1. Атака 2. Угроза 3. Уязвимость	ОПК-3.З.1
6	*Инструкция. Прочитайте задание и выберите один или несколько правильных ответов.* ЭЦП – это: 1. Электронно-цифровой преобразователь 2. Электронно-цифровая подпись 3. Электронно-цифровой процессор	ПК-6.З.1
7	Пароль пользователя должен: 1. Содержать цифры, буквы и знаки препинания 2. Быть сложным для угадывания 3. Состоять из даты рождения пользователя	ОПК-3.З.1
8	Свойствами информации, наиболее актуальными при обеспечении информационной безопасности, являются: 1. Конфиденциальность	УК-2.В.1

<table>
<tr><td></td><td>2. Доступность
3. Целостность</td><td></td></tr>
<tr><td>9</td><td>Методы аутентификации пользователей:
1. Пароль
2. Цифровой сертификат
3. Письменное заявление</td><td>ПК-6.У.1</td></tr>
<tr><td>10</td><td>Что такое идентификация?
1. Вид физической защиты
2. Процесс установления личности или объекта в системе
3. Химический процесс</td><td>ОПК-3.В.1</td></tr>
<tr><td>11</td><td>Инструкция. Прочитайте задание и расположите варианты ответа в правильной последовательности.
Расположите нарушителей информационной безопасности в порядке увеличения опасности:
1. Бывшие работники (пользователи)
2. Конкурирующие организации
3. Разработчики программных, программно-аппаратных средств
4. Специальные службы иностранных государств</td><td>ОПК-3.З.1</td></tr>
<tr><td>12</td><td>Расположите методы аутентификации в порядке увеличения надежности:
1. Пароль
2. Цифровой сертификат
3. Аппаратный токен
4. Биометрические данные</td><td>ОПК-3.В.1</td></tr>
<tr><td>13</td><td>Расположите виды информации в порядке увеличения секретности:
1. Общедоступная
2. Персональные данные
3. Коммерческая тайна
4. Государственная тайна</td><td>ПК-6.З.1</td></tr>
<tr><td>14</td><td>Расположите основные шаги по защите информации в правильном порядке:
1. Проведение оценки текущих рисков и уязвимостей
2. Разработка и внедрение политики информационной безопасности
3. Обучение сотрудников стандартам безопасности
4. Регулярное проведение аудитов и обновление мер защиты</td><td>УК-2.В.1</td></tr>
<tr><td>15</td><td>Укажите правильный порядок действий при обнаружении утечки данных:
1. Уведомление ответственных лиц и создание рабочей группы
2. Остановка утечки и ограничение доступа к затронутым системам
3. Анализ инцидента и выявление источника утечки
4. Документирование событий и разработка мероприятий по предотвращению повторения</td><td>ПК-6.У.1</td></tr>
<tr><td>16</td><td>Инструкция. Прочитайте текст и установите соответствие. К каждой позиции в левом столбце подберите соответствующую позицию в правом столбце.
Установите соответствие между примерами средств защиты и их типами:
<table><tr><td>А) Физические</td><td>1) Замок на двери</td></tr><tr><td>В) Аппаратные</td><td>2) Антивирусные программы</td></tr><tr><td>С) Программные</td><td>3) Датчики движения</td></tr></table>Запишите выбранные цифры под соответствующими буквами:
<table><tr><td>А</td><td>В</td><td>С</td></tr><tr><td></td><td></td><td></td></tr></table></td><td>УК-2.В.1</td></tr>
<tr><td>17</td><td>Установите соответствие между типами угроз и их описанием:
<table><tr><td>А) Фишинг</td><td>1) Атака, целью которой является перезагрузка или блокировка ресурса</td></tr><tr><td>В) Вредоносное ПО</td><td>2) Программа, предназначенная для нарушения работы системы или кражи данных</td></tr><tr><td>С) DDoS-атака</td><td>3) Метод обмана пользователей</td></tr></table></td><td>ПК-6.У.1</td></tr>
</table>

	для получения их конфиденциальной информации	

Запишите выбранные цифры под соответствующими буквами:

A	B	C

18	Установите соответствие между методами защиты и их описанием: A) Шифрование — 1) Процесс проверки подлинности пользователя или устройства B) Аутентификация — 2) Копирование данных для предотвращения их потери C) Бэкап — 3) Преобразование информации в недоступный для чтения формат Запишите выбранные цифры под соответствующими буквами: A | B | C	ОПК-3.З.1
19	Установите соответствие между типами данных и их описанием: A) Целочисленный — 1) Согласованное представление текста B) Строковый — 2) Значение, истинное или ложное C) Логический — 3) Целые числа без дробной части Запишите выбранные цифры под соответствующими буквами: A | B | C	ОПК-3.В.1
20	Установите соответствие между примерами средств защиты и результатами их применения: A) Использование антивирусного ПО — 1) Защита от вредоносных программ B) Регулярное обновление программного обеспечения — 2) Устранение уязвимостей и актуализация систем C) Сложные пароли — 3) Усложнение доступа к данным Запишите выбранные цифры под соответствующими буквами: A | B | C	ПК-6.З.1
21	*Инструкция. Прочитайте задание и дайте свой развернутый вариант ответа.* Перечислите основные информационные угрозы по цели (последствиям) реализации:	УК-2.В.1
22	Перечислите основные каналы утечки информации:	ОПК-3.З.1
23	Перечислите основные виды информации ограниченного доступа:	
24	Перечислите основные виды нарушителей информационной безопасности:	ПК-6.З.1

25	Перечислите основные недостатки использования парольной защиты:	ПК-6.У.1

Ответы:

1. 3
2. 2
3. 2
4. 1
5. 2
6. 2
7. 1, 2
8. 1, 2, 3
9. 1, 2
10. 2
11. 1. Бывшие работники (пользователи) 2. Конкурирующие организации 3. Разработчики программных, программно-аппаратных средств 4. Специальные службы иностранных государств
12. 1. Пароль 2. Цифровой сертификат 3. Аппаратный токен 4. Биометрические данные
13. 1. Общедоступная 2. Персональные данные 3. Коммерческая тайна 4. Государственная тайна
14. 1. Проведение оценки текущих рисков и уязвимостей 2. Разработка и внедрение политики информационной безопасности 3. Обучение сотрудников стандартам безопасности 4. Регулярное проведение аудитов и обновление мер защиты
15. 1. Уведомление ответственных лиц и создание рабочей группы 2. Остановка утечки и ограничение доступа к затронутым системам 3. Анализ инцидента и выявление источника утечки 4. Документирование событий и разработка мероприятий по предотвращению повторения
16. A) – 1; B) – 3; C) – 2
17. A) – 3; B) – 2; C) – 1
18. A) – 2; B) – 3; C) – 1
19. A) – 2; B) – 3; C) – 1
20. A) – 1; B) – 2; C) – 3
21. Основные информационные угрозы по цели (последствиям) реализации: нарушение доступности, нарушение целостности, нарушение конфиденциальности, нарушение неотказуемости, нарушение подотчетности, нарушение подлинности (аутентичности), нарушение достоверности
22. Основные каналы утечки информации: физические, визуально-оптические, технические
23. Основные виды информации ограниченного доступа: конфиденциальная, с возрастным ограничением, распространяемая владельцем по соглашению, государственная тайна
24. Основные виды нарушителей информационной безопасности: внешние или внутренние
25. Основные недостатки использования парольной защиты: слишком простой пароль, повторное его использование, утечка данных, возможность передачи пароля другому лицу, ненадлежащее хранение пароля

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.

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 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».

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

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

Система оценок при проведении текущего контроля и промежуточной аттестации осуществляется в соответствии с руководящим документом организации РДО ГУАП. СМК 3.76 «Положение о текущем контроле успеваемости и промежуточной аттестации студентов и аспирантов, обучающихся по образовательным программам высшего образования в ГУАП» https://docs.guap.ru/smk/3.76.pdf.

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