

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

ДОЦ., К.Т.Н., ДОЦ.
(должность, уч. степень, звание)

В.А. Ненашев
(инициалы, фамилия)

(подпись)
«24» июня 2024 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы информационной безопасности»
(Наименование дисциплины)

Код направления подготовки/ специальности	11.03.03
Наименование направления подготовки/ специальности	Конструирование и технология электронных средств
Наименование направленности	Проектирование и технология электронно- вычислительных средств
Форма обучения	очная
Год приема	2024

Санкт-Петербург– 2024

Лист согласования программы

Программу составил (а)

ДОЦ., К.Т.Н., ДОЦ.
(должность, уч. степень, звание)

(подпись, дата)

24.06.2024

В.А. Ненашев
(инициалы, фамилия)

Программа одобрена на заседании кафедры № 23
«24» июня 2024 г, протокол № 10/24

Заведующий кафедрой № 23

д.т.н., проф.
(уч. степень, звание)

(подпись, дата)

24.06.2024

А.Р. Бестугин
(инициалы, фамилия)

Заместитель директора института №2 по методической работе

доц., к.т.н., доц.
(должность, уч. степень, звание)

(подпись, дата)

24.06.2024

Н.В. Марковская
(инициалы, фамилия)

Аннотация

Дисциплина «Основы информационной безопасности» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 11.03.03 «Конструирование и технология электронных средств» направленности «Проектирование и технология электронно-вычислительных средств». 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»

УК-10 «Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности»

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»

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 обучающегося.

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

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

Язык обучения по дисциплине «русский»

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

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

Также целями освоения дисциплины «Основы информационной безопасности» являются раскрытие сущности и значения информационной безопасности и защиты информации, их места в системе национальной безопасности, определение теоретических, концептуальных, методологических и организационных основ обеспечения безопасности информации, классификация и характеристики составляющих информационной безопасности и защиты информации, установление взаимосвязи и логической организации входящих в них компонентов. Дисциплина входит в состав обязательной части образовательной программы высшего образования (далее – ОП ВО).

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-2.3.3 знать возможности и ограничения применения цифровых инструментов для решения поставленных задач
Универсальные компетенции	УК-10 Способен формировать нетерпимое отношение к проявлениям экстремизма, терроризма, коррупционному поведению и противодействовать им в профессиональной деятельности	УК-10.3.1 знать действующие правовые нормы, обеспечивающие противодействие коррупции, проявлениям экстремизма и терроризма в различных областях жизнедеятельности; меры по профилактике коррупции, экстремизма, терроризма

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 безопасности	ОПК-3.3.1 знает современные принципы поиска, хранения, обработки, анализа и представления в требуемом формате информации ОПК-3.В.1 владеет навыками обеспечения информационной безопасности
----------------------------------	---	--

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 как самостоятельное значение, так и используются при изучении других дисциплин:

- «Производственная преддипломная практика»,
- «ГИА».

3. Объем и трудоемкость дисциплины

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

Таблица 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№7
1	2	3
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)	36	36
Самостоятельная работа, всего (час)	57	57
Вид промежуточной аттестации: зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Экз.	Экз.

Примечание: ** кандидатский экзамен

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий.
Разделы, темы дисциплины и их трудоемкость приведены в таблице 3.

Таблица 3 – Разделы, темы дисциплины, их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 7					
Раздел 1. Введение. Цель и задачи курса	2				1
Раздел 2. Сущность и понятие информационной безопасности	4				4
Раздел 3. Значение информационной безопасности и ее место в системе национальной безопасности	4				8
Раздел 4. Сущность и понятие защиты информации	4				8
Раздел 5. Состав и классификация носителей защищаемой информации	4		4		8
Раздел 6. Понятие и структура угроз защищаемой информации	4		4		8
Раздел 7. Объекты защиты информации	4		4		10
Раздел 8. Классификация видов, методов и средств защиты информации	8		5		10
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. 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 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 Значение информационной безопасности для субъектов информационных отношений. Связь между информационной безопасностью и безопасностью информации. Понятие и современная концепция национальной безопасности. Место информационной безопасности в системе национальной безопасности.
4	Раздел 4. Сущность и понятие защиты информации Существующие подходы к

	<p>содержательной части понятия "защита информации" и способы реализации содержательной части.</p> <p>Методологическая основа раскрытия сущности и определения понятия защиты информации. Формы выражения нарушения статуса информации. Обусловленность статуса информации ее уязвимостью.</p> <p>Понятие уязвимости информации. Формы проявления уязвимости информации. Виды уязвимости информации. Понятие "утечка информации". Соотношение форм и видов уязвимости информации. Содержательная часть понятия "защита информации".</p> <p>Способ реализации содержательной части защиты информации. Определение понятия "защита информации", его соотношение с понятием, сформулированным в ГОСТ Р 50922-96. "Защита информации. Основные термины и определения".</p>
5	<p>Раздел 5. Состав и классификация носителей защищаемой информации</p> <p>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.</p> <p>Опосредованные носители защищаемой информации. Свойства и значение типов носителей защищаемой информации.</p>
6	<p>Раздел 6. Понятие и структура угроз защищаемой информации</p> <p>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.</p>
7	<p>Раздел 7. Объекты защиты информации</p> <p>Понятие объекта защиты. Носители информации как конечные объекты защиты. Особенности отдельных видов носителей как объектов защиты.</p> <p>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.</p>
8	<p>Раздел 8. Классификация видов, методов и средств защиты информации</p> <p>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.</p>

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Учебным планом не предусмотрено					
Всего					

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 6.

Таблица 6 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 7				
1	Исследование уязвимости информации	4		5
2	Исследование видов уязвимости	4		6
3	Исследование форм уязвимости	4		7
4	Построение алгоритмов социальной инженерии и способы защиты от них	5		8
Всего		17		

4.5. Курсовое проектирование/ выполнение курсовой работы
Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся
Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 7, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	30	30
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	20	20
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	7	7
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)
004.05В 75	Воронов, А. В. Основы защиты информации: учебное пособие/ А. В. Воронов, Н. В. Волошина. - СПб.: ГОУ ВПО "СПбГУАП", 2009. - 78 с.	10
004 Ш 22	Шаньгин, В. Ф. Информационная безопасность [Текст]: научно- популярная литература / В. Ф. Шаньгин. - М.: ДМК Пресс, 2014. - 702 с	10
Х Я 47	Яковец, Е. Н. Правовые основы обеспечения 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
http://www.intuit.ru/studies/courses/10/10/info	Владимир Галатенко. Основы информационной безопасности (курс лекций, с дистанционным обучением)

8. Перечень информационных технологий

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

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

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

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице 12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Мультимедийная лекционная аудитория	14-06Г

10. Оценочные средства для проведения промежуточной аттестации

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

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Экзамен	Список вопросов к экзамену; Экзаменационные билеты; Задачи; Тесты.

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

Таблица 14 –Критерии оценки уровня сформированности компетенций

Оценка компетенции 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.

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	
«хорошо» «зачтено»	<ul style="list-style-type: none"> – обучающийся твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; – не допускает существенных неточностей; – увязывает усвоенные знания с практической деятельностью направления; – аргументирует научные положения; – делает выводы и обобщения; – владеет системой специализированных понятий.
«удовлетворительно» «зачтено»	<ul style="list-style-type: none"> – обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; – допускает несущественные ошибки и неточности; – испытывает затруднения в практическом применении знаний направления; – слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий.
«неудовлетворительно» «не зачтено»	<ul style="list-style-type: none"> – обучающийся не усвоил значительной части программного материала; – допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; – испытывает трудности в практическом применении знаний; – не может аргументировать научные положения; – не формулирует выводов и обобщений.

10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора
	<p>Математические модели формальной теории защиты информации. Стандарты в области защиты информации в вычислительной системе, «Оранжевая книга» США, российские стандарты.</p> <p>Криптографические методы защиты информации. Основные понятия криптографии.</p> <p>Исторические шифры.</p> <p>Теоретическая, практическая и временная стойкость системы криптографической защиты.</p> <p>Криптографические параметры узлов и блоков шифрующих автоматов.</p> <p>Методы получения псевдослучайных последовательностей. Генераторы псевдослучайных последовательностей и их свойства. Современные потоковые и блочные алгоритмы шифрования. Системы асимметричного шифрования, открытый ключ, электронная подпись.</p> <p>Вопросы генерации и распределения ключей. Атаки на криптографические алгоритмы: алгоритмические, алгебраические, статистические. Методология обоснования надежности криптографической защиты.</p> <p>Криптографические протоколы с использованием симметричного и асимметричного шифрования.</p> <p>Криптографические протоколы с использованием цифровой подписи.</p> <p>Криптографические протоколы генерации и распределения ключей.</p> <p>Протоколы разделения секрета и доказательства без разглашения.</p>	УК-2.3.3

	<p>Протокол подбрасывания монеты по телефону. Оценка сложности арифметических операций.</p> <p>Непрерывные дроби и их свойства, квадратичные вычеты, асимптотический закон распределения простых чисел.</p> <p>Арифметические алгоритмы, (вычисление НОД, Символа Якоби), решение квадратных уравнений в конечных простых полях, алгоритмы построения и проверки простоты чисел, алгоритмы факторизации и дискретного логарифмирования.</p> <p>Криптосистема RSA, выбор параметров и взаимосвязь между ними.</p>	
	<p>Методы и средства ограничения доступа к компонентам ЭВМ.</p> <p>Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.</p> <p>Методы и средства хранения ключевой информации.</p> <p>Средства обеспечения безопасности в ОС семейства Windows и UNIX, критерии защищенности ОС.</p> <p>Средства обеспечения безопасности в сетях. Протоколы аутентификации при удаленном доступе. Средства защиты серверов и рабочих станций.</p> <p>Средства защиты локальных сетей при подключении к Internet.</p> <p>Межсетевые экраны, электронные замки, криптофильтры, крипто роутеры.</p> <p>Области применения, достоинства, недостатки, реализуемые политики безопасности.</p> <p>Методы оценки качества применяемых средств защиты. Методы и средства защиты информации в СУБД. Средства идентификации и аутентификации, управление доступом, средства контроля, аудит безопасности.</p>	ОПК-3.3.1
	<p>Критерии защищенности БД и АИС.</p> <p>Методы и системы обнаружения компьютерных атак. Экспресс-анализ защищенности сетевого компьютера от удаленных атак через сеть.</p> <p>Перечень типовых угроз вычислительной системе со стороны потенциального злоумышленника.</p> <p>Основные принципы защиты вычислительной системы от несанкционированного доступа (проверка полномочий, разграничение доступа, аудит).</p> <p>Защита информации в локальных и глобальных вычислительных сетях и ее особенности.</p> <p>Роль и задачи администратора вычислительной системы и службы безопасности.</p>	ОПК-3.В.1

Вопросы (задачи) для зачета / дифф. зачета представлены в таблице 16.

Таблица 16 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета	Код индикатора
	Учебным планом не предусмотрено	

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

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

№ п/п	Примерный перечень тем для курсового проектирования/выполнения курсовой работы
	Учебным планом не предусмотрено

Вопросы для проведения промежуточной аттестации в виде тестирования представлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	<p>- Бизнес-ориентированные, коммерческие системы</p> <p>6) Основными рисками информационной безопасности являются: Искажение, уменьшение объема, перекодировка информации Техническое вмешательство, выведение из строя оборудования сети + Потеря, искажение, утечка информации</p> <p>7) К основным принципам обеспечения информационной безопасности относятся: + Экономической эффективности системы безопасности Многоплатформенной реализации системы Усиления защищенности всех звеньев системы</p> <p>8) Основными субъектами информационной безопасности являются: руководители, менеджеры, администраторы компаний + органы права, государства, бизнеса сетевые базы данных, фаерволлы</p> <p>9) К основным функциям системы безопасности можно отнести все перечисленное: + Установление регламента, аудит системы, выявление рисков Установка новых офисных приложений, смена хостинг-компания Внедрение аутентификации, проверки контактных данных пользователей тест 10) Принципом информационной безопасности является принцип недопущения: + Неоправданных ограничений при работе в сети (системе) Рисков безопасности сети, системы Презумпции секретности</p> <p>11) Принципом политики информационной безопасности является принцип: + Невозможности миновать защитные средства сети (системы) Усиления основного звена сети, системы Полного блокирования доступа при риск-ситуациях</p> <p>12) Принципом политики информационной безопасности является принцип: + Усиления защищенности самого незащищенного звена сети (системы) Перехода в безопасное состояние работы сети, системы Полного доступа пользователей ко всем ресурсам сети, системы</p> <p>13) Принципом политики информационной безопасности является принцип: + Разделения доступа (обязанностей, привилегий) клиентам сети (системы) Одноуровневой защиты сети, системы Совместимых, однотипных программно-технических средств сети, системы</p> <p>14) К основным типам средств воздействия на компьютерную сеть относятся: Компьютерный сбой + Логические закладки («мины») Аварийное отключение питания</p> <p>15) Когда получен спам по e-mail с приложенным файлом, следует: Прочитать приложение, если оно не содержит ничего ценного – удалить Сохранить приложение в парке «Спам», выяснить затем IP- адрес генератора спама + Удалить письмо с приложением, не раскрывая (не читая) его</p> <p>16) Принцип Кирхгофа: Секретность ключа определена секретностью открытого сообщения Секретность информации определена скоростью передачи данных + Секретность закрытого сообщения определяется секретностью ключа</p> <p>17) ЭЦП – это: Электронно-цифровой преобразователь + Электронно-цифровая подпись Электронно-цифровой процессор</p> <p>18) Наиболее распространены угрозы информационной безопасности корпоративной системы: - Покупка нелегального ПО + Ошибки эксплуатации и неумышленного изменения режима работы системы - Сознательного внедрения сетевых вирусов</p> <p>19) Наиболее распространены угрозы информационной безопасности сети: Распределенный доступ клиент, отказ оборудования</p>	ОПК-3.В.1

	<p>Моральный износ сети, инсайдерство + Сбой (отказ) оборудования, нелегальное копирование данных тест_20) Наиболее распространены средства воздействия на сеть/офиса: Слабый трафик, информационный обман, вирусы в интернет + Вирусы в сети, логические мины (закладки), информационный перехват Компьютерные сбои, изменение администрирования, топологии 21) Утечкой информации в системе называется ситуация, характеризуемая: + Потерей данных в системе Изменением формы информации Изменением содержания информации 22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются: + Целостность Доступность Актуальность 23) Угроза информационной системе (компьютерной сети) – это: + Вероятное событие Детерминированное (всегда определенное) событие Событие, происходящее периодически 24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется: Регламентированной Правовой + Защищаемой 25) Разновидностями угроз безопасности (сети, системы) являются все перечисленные в списке:</p>	
--	--	--

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

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
	Не предусмотрено

10.4. Методические материалы, определяющие процедуры оценивания индикаторов, характеризующих этапы формирования компетенций, содержатся в локальных нормативных актах ГУАП, регламентирующих порядок и процедуру проведения текущего контроля успеваемости и промежуточной аттестации обучающихся ГУАП.

11. Методические указания для обучающихся по освоению дисциплины

11.1. Методические указания для обучающихся по освоению лекционного материала

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемые результаты при освоении обучающимися лекционного материала:

- получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;
- получение опыта творческой работы совместно с преподавателем;

- развитие профессионально-деловых качеств, любви к предмету и самостоятельного творческого мышления.
- появление необходимого интереса, необходимого для самостоятельной работы;
- получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;
- научиться методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);
- получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала:

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

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

11.2. Методические указания для обучающихся по выполнению лабораторных работ *(если предусмотрено учебным планом по данной дисциплине)*

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 знаний;
- Выполнение ЛР должно осуществляться на основе методических указаний, предоставляемых преподавателем;
- ЛР должна выполняться в специализированном компьютерном классе и может быть доработана студентом в домашних условиях, если позволяет ПО;
- Итогом выполненной ЛР является отчет.

Структура и форма отчета о лабораторной работе

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

Требования к оформлению отчета о лабораторной работе

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

11.3. Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Для обучающихся по заочной форме обучения, самостоятельная работа может включать в себя контрольную работу.

В процессе выполнения самостоятельной работы, у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет им развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихся являются:

- учебно-методический материал по дисциплине.

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.

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:

- экзамен – форма оценки знаний, полученных обучающимся в процессе изучения всей дисциплины или ее части, навыков самостоятельной работы, способности применять их для решения практических задач. Экзамен, как правило, проводится в период экзаменационной сессии и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Экзамен проводится в письменной форме и завершается оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично»,

«хорошо», «удовлетворительно» означают успешное прохождение экзамена. На экзамен выделяется два академических часа.

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

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

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

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

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

Оценка «отлично» выставляется при условии выполнения следующих требований:

- 1) Студент демонстрирует:
 - свободное владение терминологией;
 - высокий уровень теоретических знаний и умение использовать их для решения задач;
 - исчерпывающее последовательное, обоснованное и логически стройное изложение ответа, без ошибок;
 - демонстрируют знание современной учебной и научной литературы;
 - демонстрирует знания базовых нормативно-правовых актов;
 - демонстрируют способность к анализу и сопоставлению различных подходов к решению заявленной в билете проблематики.
- 2) Студент без затруднений ориентируется в нормативных правовых актах, научной специальной литературе.
- 3) Письменная речь студента грамотная, лаконичная, с правильной расстановкой акцентов.

Оценка «хорошо» выставляется при условии выполнения следующих требований:

- 1) Студент демонстрирует:
 - владение терминологией на достаточном уровне;
 - достаточный уровень теоретических знаний и умение использовать их для

решения задач;

- грамотное и логичное изложение ответа, без существенных ошибок, но изложение недостаточно систематизировано и последовательно.

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

3) Письменная речь студента грамотная, лаконичная, с правильной речевой интонацией.

Оценка «удовлетворительно» выставляется при условии выполнения следующих требований:

1) Студент демонстрирует:

- владение терминологией на минимальном уровне;
- низкий пороговый уровень теоретических знаний, усвоил только основной программный материал без знания отдельных особенностей;

- при ответе допускает неточности, материал недостаточно систематизирован;
- нарушения в последовательности изложения.

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

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

Оценка «неудовлетворительно» выставляется при условии:

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

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

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой