

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ
ФЕДЕРАЦИИ

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

Кафедра № 33

УТВЕРЖДАЮ
Руководитель направления

А.Ф. - И. В. ДИ.

(подпись, и.о. имени, фамилия)

А.О. Смирнов

(подпись, фамилия)

и.о. имени

«26» мая 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Информационная безопасность»
(наименование дисциплины)

Лист составления рабочей программы дисциплины

Программу составил (я)

А.Т.И. - ДИ.

(подпись, и.о. имени, фамилия)

26.05.22

(подпись, и.о. имени)

С.Н. Бегитов

(подпись, фамилия)

Программа одобрена на заседании кафедры № 33

«26» мая 2022 г. протокол № 10

Заведующий кафедрой № 33

А.Т.И. - ДИ.

(подпись, и.о. имени, фамилия)

26.05.22

(подпись, и.о. имени)

С.Н. Бегитов

(подпись, фамилия)

Ответственный за ОП ВО 01.03.02(01)

А.О. - И. В. ДИ.

(подпись, и.о. имени, фамилия)

26.05.22

(подпись, и.о. имени)

А.О. Смирнов

(подпись, фамилия)

Заместитель декана факультета №1 по учебно-методической работе

И.И. - И. В. ДИ.

(подпись, и.о. имени, фамилия)

26.05.22

(подпись, и.о. имени)

Р.Н. Цылис

(подпись, фамилия)

Код направления подготовки/ специальности	01.03.02
Наименование направления подготовки/ специальности	Прикладная математика и информатика
Наименование направленности	Прикладная математика и информатика в наукоемком производстве
Форма обучения	очная

Аннотация

Дисциплина «Информационная безопасность» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/специальности 01.03.02 «Прикладная математика и информатика» направленности «Прикладная математика и информатика в наукоемком производстве». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ОПК-4 «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, практические работы, самостоятельная работа студента, консультации.

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

Общая трудоемкость освоения дисциплины составляет 5 зачетных единиц, 180 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
Общепрофессиональные компетенции	ОПК-4 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-4.3.1 знать перспективные методы информационных технологий и искусственного интеллекта, направленные на разработку новых научно-технических решений ОПК-4.У.1 уметь применять современные информационные технологии и перспективные методы искусственного интеллекта для решения задач профессиональной деятельности с учетом требований информационной безопасности ОПК-4.В.1 владеть навыками разработки алгоритмов решения задач в профессиональной деятельности

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 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)	5/ 180	5/ 180
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)	93	93
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	2				9
Раздел 2. Сущность и понятие информационной безопасности	4				12
Раздел 3. Значение информационной безопасности и ее место в системе национальной безопасности	4				12
Раздел 4. Сущность и понятие защиты информации	4				12
Раздел 5. Состав и классификация носителей защищаемой информации	4		4		12
Раздел 6. Понятие и структура угроз защищаемой информации	4		4		12
Раздел 7. Объекты защиты информации	4		4		12
Раздел 8. Классификация видов, методов и средств защиты информации	8		5		12
Итого в семестре:	34	0	17		93
Итого	34	0	17	0	93

Практическая подготовка заключается в непосредственном выполнении обучающимися определенных трудовых функций, связанных с будущей профессиональной деятельностью.

4.2. Содержание разделов и тем лекционных занятий.

Содержание разделов и тем лекционных занятий приведено в таблице 4.

Таблица 4 – Содержание разделов и тем лекционного цикла

Номер раздела	Название и содержание разделов и тем лекционных занятий
1	<p><i>Раздел 1. Введение.</i></p> <p>Предмет и задачи курса. Значение и место курса в, подготовке специалистов, по защите информации. Научная и учебная взаимосвязь курса с другими дисциплинами. Разделы и темы, их распределение по видам аудиторных занятий. Формы проведения семинарских занятий. Состав и методика самостоятельной работы студентов по изучению дисциплины. Формы проверки знаний. Анализ нормативных источников, научной и учебной литературы. Знания и умения студентов, которые должны быть получены в результате изучения курса.</p>
2	<p><i>Раздел 2. Сущность и понятие информационной безопасности</i></p> <p>Становление и развитие понятия "информационная безопасность". Современные подходы к определению понятия. Сущность информационной безопасности. Объекты информационной безопасности. Связь информационной безопасности с информатизацией общества. Структура информационной безопасности. Определение понятия информационная безопасность".</p>
3	<p><i>Раздел 3. Значение информационной безопасности и ее место в системе национальной безопасности</i></p> <p>Значение информационной, безопасности для субъектов информационных отношений.</p> <p>Связь между информационной безопасностью и безопасностью информации.</p> <p>Понятие и современная концепция национальной безопасности. Место информационной, безопасности, в системе национальной безопасности.</p>
4	<p><i>Раздел 4. Сущность и понятие защиты информации</i></p> <p>Существующие подходы к 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><i>Раздел 5. Состав и классификация носителей защищаемой информации</i></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. Опосредованные носители защищаемой</p>

	информации. Свойства и значение типов носителей защищаемой информации.
6	<i>Раздел 6. Понятие и структура угроз защищаемой информации</i> Современные подходы к понятию угрозы защищаемой информации. Связь угрозы защищаемой информации с уязвимостью информации. Признаки и составляющие угрозы: явления, факторы, условия. Понятие угрозы защищаемой информации. Структура явлений как сущностного выражения угрозы защищаемой информации. Структура факторов, создающих возможность дестабилизирующего воздействия на информацию.
7	<i>Раздел 7. Объекты защиты информации</i> Понятие объекта защиты. Носители информации как конечные объекты защиты. Особенности отдельных видов носителей как объектов защиты. Состав объектов хранения письменных и видовых носителей информации, подлежащих защите. Состав подлежащих защите технических средств отображения, обработки, хранения, воспроизведения передачи информации. Другие объекты защиты информации. Виды и способы дестабилизирующего воздействия на объекты защиты.
8	<i>Раздел 8. Классификация видов, методов и средств защиты информации</i> 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 8				
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)	60	60
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	13	13
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)	20	20
Всего:	93	93

5. Перечень учебно-методического обеспечения
для самостоятельной работы обучающихся по дисциплине (модулю)
Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. 7-11.

6. Перечень печатных и электронных учебных изданий
Перечень печатных и электронных учебных изданий приведен в таблице 8.
Таблица 8– Перечень печатных и электронных учебных изданий

Шифр/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
004.05В 75	Воронов, А. В. Основы защиты информации: учебное пособие/ А. В. Воронов, Н. В. Волошина. - СПб.: ГОУ ВПО "СПбГУАП", 2009. - 78 с.	
004 III 22	Шаньгин, В. Ф. Информационная безопасность [Текст]: научно-популярная литература / В. Ф. Шаньгин. - М.: ДМК Пресс, 2014. - 702 с	

Х Я 47	Яковец, Е. Н. Правовые основы обеспечения информационной безопасности Российской Федерации [Текст] : учебное пособие / Е. Н. Яковец. - М. : Юрлитинформ, 2010. - 336 с.	
	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	Лекционная аудитория	
2	Компьютерный класс	

10. Оценочные средства для проведения промежуточной аттестации

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

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Экзамен	Список вопросов к экзамену; 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»	<ul style="list-style-type: none"> – 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»	<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.

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	
«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
1	<p>Математические модели формальной теории защиты информации.</p> <p>Стандарты в области защиты информации в вычислительной системе, «Оранжевая книга» США, российские стандарты.</p> <p>Криптографические методы защиты информации.</p> <p>Основные понятия криптографии.</p> <p>Исторические шифры.</p> <p>Теоретическая, практическая и временная стойкость системы криптографической защиты.</p> <p>Криптографические параметры узлов и блоков шифрующих автоматов.</p> <p>Методы получения псевдослучайных последовательностей.</p> <p>Генераторы псевдослучайных последовательностей и их свойства.</p> <p>Современные поточные и блочные алгоритмы шифрования.</p> <p>Системы асимметричного шифрования, открытый ключ, электронная подпись.</p> <p>Вопросы генерации и распределения ключей.</p> <p>Атаки на криптографические алгоритмы: алгоритмические, алгебраические, статистические.</p> <p>Методология обоснования надежности криптографической защиты.</p> <p>Криптографические протоколы с использованием симметричного и асимметричного шифрования.</p> <p>Криптографические протоколы с использованием цифровой подписи.</p>	ОПК-4.3.1

	<p>Криптографические протоколы генерации и распределения ключей.</p> <p>Протоколы разделения секрета и доказательства без разглашения.</p> <p>Протокол подбрасывания монеты по телефону.</p> <p>Оценка сложности арифметических операций.</p> <p>Непрерывные дроби и их свойства, квадратичные вычеты, асимптотический закон распределения простых чисел.</p> <p>Арифметические алгоритмы, (вычисление НОД, Символа Якоби), решение квадратных уравнений в конечных простых полях, алгоритмы построения и проверки простоты чисел, алгоритмы факторизации и дискретного логарифмирования.</p> <p>Криптосистема RSA, выбор параметров и взаимосвязь между ними.</p>	
2	<p>Методы и средства ограничения доступа к компонентам ЭВМ.</p> <p>Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.</p> <p>Методы и средства хранения ключевой информации.</p> <p>Средства обеспечения безопасности в ОС семейств Windows и UNIX, критерии защищенности ОС.</p> <p>Средства обеспечения безопасности в сетях.</p> <p>Протоколы аутентификации при удаленном доступе.</p> <p>Средства защиты серверов и рабочих станций.</p> <p>Средства защиты локальных сетей при подключении к Internet.</p>	ОПК-4.У.1
3	<p>Межсетевые экраны, электронные замки, криптофильтры, криптороутеры.</p> <p>Области применения, достоинства, недостатки, реализуемые политики безопасности.</p> <p>Методы оценки качества применяемых средств защиты.</p> <p>Методы и средства защиты информации в СУБД.</p> <p>Средства идентификации и аутентификации, управление доступом, средства контроля, аудит безопасности.</p> <p>Критерии защищенности БД и АИС.</p> <p>Методы и системы обнаружения компьютерных атак.</p> <p>Экспресс-анализ защищенности сетевого компьютера от удаленных атак через сеть.</p> <p>Перечень типовых угроз вычислительной системе со стороны потенциального злоумышленника.</p> <p>Основные принципы защиты вычислительной системы от несанкционированного доступа (проверка полномочий, разграничение доступа, аудит).</p> <p>Защита информации в локальных и глобальных вычислительных сетях и ее особенности.</p> <p>Роль и задачи администратора вычислительной системы и службы безопасности.</p>	ОПК-4.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
1	<p>Компьютер Боба заражен вирусом, который непрерывно размножается. Одну миллисекунду вновь рожденный вирус обживает, а затем каждую следующую миллисекунду производит новую копию самого себя. Все началось с одной единственной копии. Боб обратился за помощью к Тренту, и тот нашел ошибку в программе вируса. Оказывается, что, как только количество копий станет кратно 2^{32}, все они будут мгновенно уничтожены, и компьютер будет спасен. Стоит ли Бобу надеяться на спасение? Если да, то как долго придется ждать?</p> <p>Боб использует в качестве пароля случайную десятичную строку длины n. Пароль вводится на сенсорном устройстве Suxen. Виктор может разглядеть отпечатки пальцев Боба и узнать, сколько в пароле нулей, единиц, двоек и так далее. Виктор может воспользоваться наблюдениями и уменьшить число паролей, которые требуется проверить. Если, например, Виктор знает, что в пароле ровно одна единица, то ему требуется проверить не 10^n, а только $n \cdot 9^{n-1}$ паролей. Во сколько раз уменьшается среднее число паролей, которые требуется проверить Виктору?</p> <p>10 символов русского и английского алфавитов имеют одинаковое начертание. Это А, В, Е, К, М, Н, О, Р, Т, Х. Виктор открыл агенство по регистрации имен в доменной зоне Трента. На самом деле Виктор готовится к омографической атаке. Он ищет одинаково записываемые слова (доменные имена), осмысленные и в русском, и в английских языках. Первое из найденных им слов: МОРЕ. Виктор собирается предложить Бобу зарегистрировать русское доменное имя и одновременно самому зарегистрировать английский зеркальный аналог. Виктор добивается того, чтобы пользователи сайта Боба вводили пароли на зеркале Виктора. Найдите как можно больше подходящих русско-английских слов, чтобы помочь Тренту составить словарь запрещенных доменных имен и тем самым защититься от атаки Виктора.</p> <p>Замок чемодана запирается 4-значным десятичным кодом. Цифры кода задются 4 роторами. Для подбора кода Виктор поворачивает некоторый из роторов либо по часовой стрелке, либо против часовой, увеличивая либо уменьшая на 1 (по модулю 10) цифру ротора. Каждый набранный на роторах код сравнивается с истинным. В случае совпадения замок отпирается. В случае несовпадения Виктор может поворачивать роторы и дальше. Может ли Виктор гарантированно открыть замок после 9999 поворотов? Если да, то как он должен действовать. Вначале замок закрыт.</p>	ОПК-4.У.1

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

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

№ п/п	Примерный перечень тем для курсового проектирования/выполнения
-------	--

	курсовой работы
	Учебным планом не предусмотрено

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

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	<p>1) К правовым методам, обеспечивающим информационную безопасность, относятся:</p> <ul style="list-style-type: none"> - Разработка аппаратных средств обеспечения правовых данных - Разработка и установка во всех компьютерных правовых сетях журналов учета действий + Разработка и конкретизация правовых нормативных актов обеспечения безопасности <p>2) Основными источниками угроз информационной безопасности являются все указанное в списке:</p> <ul style="list-style-type: none"> - Хищение жестких дисков, подключение к сети, инсайдерство + Перехват данных, хищение данных, изменение архитектуры системы - Хищение данных, подкуп системных администраторов, нарушение регламента работы <p>3) Виды информационной безопасности:</p> <ul style="list-style-type: none"> + Персональная, корпоративная, государственная - Клиентская, серверная, сетевая - Локальная, глобальная, смешанная <p>4) Цели информационной безопасности – своевременное обнаружение, предупреждение:</p> <ul style="list-style-type: none"> + несанкционированного доступа, воздействия в сети - инсайдерства в организации - чрезвычайных ситуаций <p>5) Основные объекты информационной безопасности:</p> <ul style="list-style-type: none"> + Компьютерные сети, базы данных - Информационные системы, психологическое состояние пользователей - Бизнес-ориентированные, коммерческие системы <p>6) Основными рисками информационной безопасности являются:</p> <ul style="list-style-type: none"> - Искажение, уменьшение объема, перекодировка информации - Техническое вмешательство, выведение из строя оборудования сети + Потеря, искажение, утечка информации <p>7) К основным принципам обеспечения информационной безопасности относится:</p> <ul style="list-style-type: none"> + Экономической эффективности системы безопасности - Многоплатформенной реализации системы - Усиления защищенности всех звеньев системы <p>8) Основными субъектами информационной безопасности являются:</p> <ul style="list-style-type: none"> - руководители, менеджеры, администраторы компаний + органы права, государства, бизнеса - сетевые базы данных, фаерволлы 	ОПК-4.У.1

	<p>9) К основным функциям системы безопасности можно отнести все перечисленное:</p> <ul style="list-style-type: none"> + Установление регламента, аудит системы, выявление рисков - Установка новых офисных приложений, смена хостинг-компания - Внедрение аутентификации, проверки контактных данных пользователей <p>тест 10) Принципом информационной безопасности является принцип недопущения:</p> <ul style="list-style-type: none"> + Неоправданных ограничений при работе в сети (системе) - Рисков безопасности сети, системы - Презумпции секретности <p>11) Принципом политики информационной безопасности является принцип:</p> <ul style="list-style-type: none"> + Невозможности миновать защитные средства сети (системы) - Усиления основного звена сети, системы - Полного блокирования доступа при риск-ситуациях <p>12) Принципом политики информационной безопасности является принцип:</p> <ul style="list-style-type: none"> + Усиления защищенности самого незащищенного звена сети (системы) - Перехода в безопасное состояние работы сети, системы - Полного доступа пользователей ко всем ресурсам сети, системы <p>13) Принципом политики информационной безопасности является принцип:</p> <ul style="list-style-type: none"> + Разделения доступа (обязанностей, привилегий) клиентам сети (системы) - Одноуровневой защиты сети, системы - Совместимых, однотипных программно-технических средств сети, системы <p>14) К основным типам средств воздействия на компьютерную сеть относится:</p> <ul style="list-style-type: none"> - Компьютерный сбой + Логические закладки («мины») - Аварийное отключение питания <p>15) Когда получен спам по e-mail с приложенным файлом, следует:</p> <ul style="list-style-type: none"> - 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>16) Принцип Кирхгофа:</p> <ul style="list-style-type: none"> - Секретность ключа определена секретностью открытого сообщения - Секретность информации определена скоростью передачи данных + Секретность закрытого сообщения определяется секретностью ключа <p>17) ЭЦП – это:</p> <ul style="list-style-type: none"> - Электронно-цифровой преобразователь + Электронно-цифровая подпись - Электронно-цифровой процессор <p>18) Наиболее распространены угрозы информационной безопасности корпоративной системы:</p>	
--	---	--

<p>- Покупка нелегального ПО</p> <p>+ Ошибки эксплуатации и неумышленного изменения режима работы системы</p> <p>- Сознательного внедрения сетевых вирусов</p> <p>19) Наиболее распространены угрозы информационной безопасности сети:</p> <p>- Распределенный доступ клиент, отказ оборудования</p> <p>- Моральный износ сети, инсайдерство</p> <p>+ Сбой (отказ) оборудования, нелегальное копирование данных</p> <p>тест_20) Наиболее распространены средства воздействия на сеть офиса:</p> <p>- Слабый трафик, информационный обман, вирусы в интернет</p> <p>+ Вирусы в сети, логические мины (закладки), информационный перехват</p> <p>- Компьютерные сбои, изменение администрирования, топологии</p> <p>21) Утечкой информации в системе называется ситуация, характеризующаяся:</p> <p>+ Потерей данных в системе</p> <p>- Изменением формы информации</p> <p>- Изменением содержания информации</p> <p>22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:</p> <p>+ Целостность</p> <p>- Доступность</p> <p>- Актуальность</p> <p>23) Угроза информационной системе (компьютерной сети) – это:</p> <p>+ Вероятное событие</p> <p>- Детерминированное (всегда определенное) событие</p> <p>- Событие, происходящее периодически</p> <p>24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:</p> <p>- Регламентированной</p> <p>- Правовой</p> <p>+ Защищаемой</p> <p>25) Разновидностями угроз безопасности (сети, системы) являются все перечисленные в списке:</p> <p>+ Программные, технические, организационные, технологические</p> <p>- Серверные, клиентские, спутниковые, наземные</p> <p>- Личные, корпоративные, социальные, национальные</p> <p>26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:</p> <p>+ Владелец сети</p> <p>- Администратор сети</p> <p>- Пользователь сети</p> <p>27) Политика безопасности в системе (сети) – это комплекс:</p> <p>+ Руководств, требований обеспечения необходимого уровня безопасности</p> <p>- Инструкций, алгоритмов поведения пользователя в сети</p> <p>- Нормы информационного права, соблюдаемые в сети</p> <p>28) Наиболее важным при реализации защитных мер политики безопасности является:</p> <p>- Аудит, анализ затрат на проведение защитных мер</p>	
---	--

	- Аудит, анализ безопасности + Аудит, анализ уязвимостей, риск-ситуаций	
--	--	--

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

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
	Не предусмотрено

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

11. Методические указания для обучающихся по освоению дисциплины

11.1. Методические указания для обучающихся по освоению лекционного материала

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

Планируемые результаты при освоении обучающимися лекционного материала:

- получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;
- получение опыта творческой работы совместно с преподавателем;
- развитие профессионально-деловых качеств, любви к предмету и самостоятельного творческого мышления.
- появление необходимого интереса, необходимого для самостоятельной работы;
- получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;
- научиться методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);
- получение точного понимания всех необходимых терминов и понятий.

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

Структура предоставления лекционного материала:

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

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

11.2. Методические указания для обучающихся по выполнению лабораторных работ

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом, и относится к средствам, обеспечивающим решение следующих основных задач обучающегося:

- приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;
- закрепление, развитие и детализация теоретических знаний, полученных на лекциях;
- получение новой информации по изучаемой дисциплине;
- приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание и требования к проведению лабораторных работ

- В задании должно быть четко сформулирована задача, выполняемая в ЛР;
- Описаны входные и выходные данные для проведения ЛР;
- ЛР должна выполняться на основе полученных теоретических знаниях;
- Выполнение ЛР должно осуществляться на основе методических указаний, предоставляемых преподавателем;
- ЛР должна выполняться в специализированном компьютерном классе и может быть доработана студентом в домашних условиях, если позволяет ПО;
- Итогом выполненной ЛР является отчет.

Структура и форма отчета о лабораторной работе

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

Требования к оформлению отчета о лабораторной работе

- Лабораторная работа (ЛР) предоставляется в печатном/или электронном виде;
- ЛР должна соответствовать структуре и форме отчета представленной выше;
- ЛР должна иметь титульный лист (ГОСТ 7.32-2001 издания 2008 года) с названием и подписью студента(ов), который(ые) ее сделал(и) и оформил(и);

Студент должен защитить ЛР. Отметка о защите должна находиться на титульном листе вместе с подписью преподавателя.

11.3. Методические указания для обучающихся по прохождению самостоятельной работы

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

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

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

Методическими материалами, направляющими самостоятельную работу обучающихся являются:

- учебно-методический материал по дисциплине;
- методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

11.4. Методические указания для обучающихся по прохождению промежуточной аттестации.

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

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

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

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

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

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

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

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

Оценка «отлично» выставляется при условии выполнения следующих требований:

1) Студент демонстрирует:

- свободное владение терминологией;
- высокий уровень теоретических знаний и умение использовать их для решения задач;

- исчерпывающее последовательное, обоснованное и логически стройное изложение ответа, без ошибок;
 - демонстрируют знание современной учебной и научной литературы;
 - демонстрирует знания базовых нормативно-правовых актов;
 - демонстрируют способность к анализу и сопоставлению различных подходов к решению заявленной в билете проблематики.
- 2) Студент без затруднений ориентируется в нормативных правовых актах, научной и иной специальной литературе.
 - 3) Письменная речь студента грамотная, лаконичная, с правильной расстановкой акцентов.

Оценка «хорошо» выставляется при условии выполнения следующих требований:

- 1) Студент демонстрирует:
 - владение терминологией на достаточном уровне;
 - достаточный уровень теоретических знаний и умение использовать их для решения задач;
 - грамотное и логичное изложение ответа, без существенных ошибок, но изложение недостаточно систематизировано и последовательно.
- 2) Студент с некоторыми затруднениями ориентируется в нормативных правовых актах, научной и иной специальной литературе.
- 3) Письменная речь студента грамотная, лаконичная, с правильной расстановкой акцентов.

Оценка «удовлетворительно» выставляется при условии выполнения следующих требований:

- 1) Студент демонстрирует:
 - владение терминологией на минимальном уровне;
 - низкий пороговый уровень теоретических знаний, усвоил только основной программный материал без знания отдельных особенностей;
 - при ответе допускает неточности, материал недостаточно систематизирован;
 - нарушения в последовательности изложения.
- 2) Студент с затруднениями ориентируется в нормативных правовых актах, научной и иной специальной литературе.
- 3) Письменная речь студента в основном грамотная, но не демонстрируется уверенное владение материалом.

Оценка «неудовлетворительно» выставляется при условии:

- 1) Студент не владеет профессиональной терминологией, демонстрирует низкий уровень теоретических знаний и умения использовать их для решения задач.
- 2) Студент не знает значительной части программного материала, допускает существенные грубые ошибки, не ориентируется в нормативных правовых актах, научной и иной специальной литературе.

Лист внесения изменений в рабочую программу дисциплины

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