МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ–ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

Кафедра №51

«УТВЕРЖДАЮ»
Руководитель направления
проф.,д.т.н.,доц.
(должность, уч. степень, звание)
С.В. Беззатеев
(подпись)
«24» июня 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы информационной безопасности»
(Название дисциплины)

Код направления	10.05.03
Наименование направления/ специальности	Информационная безопасность автоматизированных систем
Наименование направленности	Обеспечение информационной безопасности распределенных информационных систем
Форма обучения	очная

Санкт-Петербург 2021 г.

Лист согласования рабочей программы дисциплины

Программу составил (а)

зав.каф., к.т.н., доц.	24.06.2021	А.А. Овчинников
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Программа одобрена на заседании кафедры № 51

«24» июня 2021 г, протокол №11

Заведующий кафедрой № 51

к.т.н.,доц.	24.06.2021	А.А. Овчинников
(уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Ответственный за ОП 10.05.03(07)

доц.,к.т.н.,доц.	24.06.2021	В.А. Мыльников
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Заместитель директора института №3 по методической работе

доц.,к.э.н.,доц.	24.06.2021	Г.С. Армашова-Тельник
(должность, уч. степень, звание)	(подпись, дата)	(инициалы, фамилия)

Аннотация

Дисциплина «Основы информационной безопасности» входит в базовую часть образовательной программы подготовки обучающихся по специальности 10.05.03 «Информационная безопасность автоматизированных систем» направленность «Обеспечение информационной безопасности распределенных информационных систем». Дисциплина реализуется кафедрой №51.

Дисциплина нацелена на формирование у выпускника

общепрофессиональных компетенций:

ОПК-4 «способность понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах»;

профессиональных компетенций:

ПК-6 «способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности»,

ПК-11 «способность разрабатывать политику информационной безопасности автоматизированной системы».

Содержание дисциплины охватывает круг вопросов, связанных с 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, практические занятия, самостоятельная работа студента, консультации.

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

Целью освоения дисциплины «Основы информационной безопасности» является раскрытие сущности и значения информационной безопасности и защиты информации, ее место 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. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:
ОПК-4 «способность понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах»:

знать – современные информационные технологии, применяемые для поиска информации в компьютерных системах, сетях, библиотечных фондах
уметь – применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах
владеть навыками – поиска информации в компьютерных системах, сетях, библиотечных фондах с помощью современных информационных технологий
иметь опыт деятельности – поиска информации в компьютерных системах, сетях, библиотечных фондах;

ПК-6 «способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности»:

знать – методы анализа, оптимизации при выборе решений по обеспечению эффективного применения автоматизированных систем в сфере обеспечения информационной безопасности
уметь – проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере обеспечения информационной безопасности
владеть навыками – анализа при выборе эффективного применения автоматизированных систем в сфере профессиональной деятельности
иметь опыт деятельности – выбора решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности;

ПК-11 «способность разрабатывать политику информационной безопасности автоматизированной системы»:

знать – виды угроз безопасности информации и возможные методы реализации угроз на основе анализа структуры и содержания информационных процессов и особенностей функционирования компьютерных сетей;
уметь – поддерживать выполнение комплекса мер по обеспечению защиты сетей от несанкционированного доступа;
владеть навыками – анализа структуры и содержания информационных процессов в компьютерных сетях и особенностей защиты сетей от несанкционированного доступа;
иметь опыт деятельности – в применении методов защиты сетей от несанкционированного доступа на практике.

2. Место дисциплины в структуре ОП

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

- Информатика;
- Математическая логика и теория алгоритмов.

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

- Программно-аппаратные средства обеспечения информационной безопасности;
- Управление информационной безопасностью;
- Техническая защита информации.

3. Объем дисциплины в ЗЕ/академ. час

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 1

Таблица 1 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№2
1	2	3
Общая трудоемкость дисциплины, ЗЕ/(час)	4/ 144	4/ 144
Из них часов практической подготовки	22	22
Аудиторные занятия, всего час., ***В том числе***	51	51
Лекции (Л), (час)	17	17
Практические/семинарские занятия (ПЗ), (час)	17	17
Лабораторные работы (ЛР), (час)	17	17
Курсовой проект (работа) (КП, КР), (час)		
Экзамен, (час)	36	36
Самостоятельная работа, всего (час)	57	57
Вид промежуточного контроля: зачет, дифф. зачет, экзамен **(Зачет, Дифф. зач, Экз.)**	Экз.	Экз.

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий

Разделы и темы дисциплины и их трудоемкость приведены в таблице 2.

Таблица 2. – Разделы, темы дисциплины и их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП (час)	СРС (час)
Семестр 2					
Раздел 1. Введение	2	1	1		3
Раздел 2.Сущность и понятие информационной безопасности	2	2	2		7
Раздел 3. Значение информационной безопасности и ее место в системе национальной безопасности	2	2	2		6

Раздел 4. Сущность и понятие защиты информации	2	2	2		6
Текущий контроль	1				7
Раздел 5. Состав и классификация носителей защищаемой информации	2	4	4		8
Раздел 6. Понятие и структура угроз защищаемой информации	2	2	2		6
Раздел 7. Объекты защиты информации	2	2	2		6
Раздел 8. Классификация видов, методов и средств защиты информации	2	2	2		8
Итого в семестре:	17	17	17		57
Итого:	17	17	17		57

4.2. Содержание разделов и тем лекционных занятий

Содержание разделов и тем лекционных занятий приведено в таблице 3.

Таблица 3 - Содержание разделов и тем лекционных занятий

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 содержательной части понятия "защита информации" и способы реализации содержательной части. Методологическая основа раскрытия сущности и определения понятия защиты информации. Формы выражения нарушения статуса информации. Обусловленность статуса информации ее уязвимостью. Понятие уязвимости информации. Формы проявления уязвимости информации. Виды уязвимости информации. Понятие "утечка информации". Соотношение форм и видов уязвимости информации. Содержательная часть понятия "защита информации". Способ реализации содержательной части защиты информации. Определение понятия "защита информации", его соотношение с понятием, сформулированным в ГОСТ Р 50922-96. "Защита информации. Основные термины и определения".
5	*Раздел 5. Состав и классификация носителей защищаемой информации* Понятие носитель защищаемой информации". Соотношение между носителем и источником информации. Состав носителей защищаемой информации. Способы фиксирования информации в носителях. Виды отображения информации в носителях. Методы воспроизведения отображенной информации в носителях информации. Носители письменной, видовой, излучаемой информации. Опосредованные носители защищаемой информации. Свойства и значение типов носителей защищаемой информации.
6	*Раздел 6. Понятие и структура угроз защищаемой информации* Современные подходы к понятию угрозы защищаемой информации. Связь угрозы защищаемой информации с уязвимостью информации. Признаки и составляющие угрозы: явления, факторы, условия. Понятие угрозы защищаемой информации. Структура явлений как сущностного выражения угрозы защищаемой информации. Структура факторов, создающих возможность дестабилизирующего воздействия на информацию.
7	*Раздел 7. Объекты защиты информации* 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	*Раздел 8. Классификация видов, методов и средств защиты информации* 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 4.

Таблица 4 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 2					
1	Задачи информационной безопасности	групповая дискуссия	3		1
2	Исторические шифры	решение ситуационных задач	3		2
3	Блоковые шифры	решение ситуационных задач	2		2
4	Математические основы систем с открытым ключом	решение ситуационных задач	2		3
5	Основные алгоритмы с открытым ключом	решение ситуационных задач	3		3
6	Основные протоколы с открытым ключом	занятие по моделированию реальных условий	2	2	4
7	Специальные протоколы	деловая учебная игра	2	2	4
Всего:			17	4	

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
1.	Исследование генераторов паролей с заданными требованиями	2	2	2
2.	Построение модели угроз информационной системы	2	2	3
3.	Построение модели утечки информационной безопасности	2	2	4
4.	Исследование уязвимости информации	1	1	4
5.	Исследование видов уязвимости	1	1	5
6.	Исследование форм уязвимости	1	1	5
7.	Построение алгоритмов социальной инженерии и способы защиты от них	1	1	6
8.	Построение алгоритмов принятия решения	1	1	6

9.	Анализ обрабатываемой информации с точки зрения видов тайн и формирование требований к ее защите	2	2	7
10.	Анализ обрабатываемой информации с точки зрения ее защиты	2	2	8
11.	Сравнение криптографических и технических средств защиты.	2	2	8
	Всего:	17	17	

4.5. Курсовое проектирование (работа)

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 6.

Таблица 6 Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 2, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	27	27
Расчетно-графическое задание (РГЗ)	20	20
Подготовка к текущему контролю успеваемости (ТКУ)	10	10
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. 8-10.

6. Перечень основной и дополнительной литературы

6.1. Основная литература

Перечень основной литературы приведен в таблице 7.

Таблица 7 – Перечень основной литературы

Шифр	Библиографическая ссылка / URL адрес	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.	СО (74)
	Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : учебное пособие. — Электрон. дан. — М. : ДМК Пресс, 2012. — 592 с http://e.lanbook.com/books/element.php?pl1_id=3032	

6.2. Дополнительная литература

Перечень дополнительной литературы приведен в таблице 8.

Таблица 8 – Перечень дополнительной литературы

Шифр	Библиографическая ссылка/ URL адрес	Количество экземпляров в библиотеке (кроме электронных экземпляров)
	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. http://e.lanbook.com/books/element.php?pl1_id=4959	

7. Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень ресурсов информационно-телекоммуникационной сети ИНТЕРНЕТ, необходимых для освоения дисциплины

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, используемых при осуществлении образовательного процесса по дисциплине

8.1.Перечень программного обеспечения

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10 – Перечень программного обеспечения

№ п/п	Наименование
1	MS Windows
2	MS Office
3	Инструментальная среда программирования

8.2.Перечень информационно-справочных систем

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11 – Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Состав материально-технической базы представлен в таблице 12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)

1	Фонд аудиторий ГУАП для проведения занятий лекционного и семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Специализированная мебель; технические средства обучения, служащие для представления учебной информации большой аудитории; переносной набор демонстрационного оборудования	
2	Вычислительная лаборатория Специализированная мебель; технические средства обучения, служащие для представления учебной информации большой аудитории; лабораторное оборудование (ПЭВМ - 12 шт., объединенных в локальную вычислительную сеть с выходом в вычислительную сеть ГУАП и Интернет)	

10. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

10.1. Состав фонда оценочных средств приведен в таблице 13

Таблица 13 - Состав фонда оценочных средств для промежуточной аттестации

Вид промежуточной аттестации	Примерный перечень оценочных средств
Экзамен	Список вопросов к экзамену; Задания.

10.2. Перечень компетенций, относящихся к дисциплине, и этапы их формирования в процессе освоения образовательной программы приведены в таблице 14.

Таблица 14 – Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Номер семестра	Этапы формирования компетенций по дисциплинам/практикам в процессе освоения ОП
ОПК-4 «способность понимать значение информации в развитии современного общества, применять достижения современных информационных технологий для поиска информации в компьютерных системах, сетях, библиотечных фондах»	
1	Информатика
2	Основы программирования
2	Безопасность жизнедеятельности
2	Основы информационной безопасности
2	Учебная ознакомительная практика
3	Основы программирования
3	Информационные технологии
4	Технологии и методы программирования
4	Учебная практика учебно-лабораторный практикум
5	Теория информации
6	Теория информационной безопасности
6	Производственная эксплуатационная практика
6	Моделирование систем

7	Техническая защита информации
8	Языки программирования
8	Защита информации в распределенных информационных системах
8	Производственная конструкторская практика
9	Производственная практика научно-исследовательская работа
10	Производственная практика научно-исследовательская работа
10	Технология построения защищенных распределенных приложений
10	Информационная безопасность распределенных информационных систем
10	Производственная преддипломная практика
ПК-6 «способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности»	
2	Основы информационной безопасности
7	Безопасность сетей ЭВМ
7	Безопасность систем баз данных
7	Техническая защита информации
7	Безопасность операционных систем
9	Разработка мобильных приложений
ПК-11 «способность разрабатывать политику информационной безопасности автоматизированной системы»	
2	Основы информационной безопасности
5	Стандарты информационной безопасности
7	Безопасность операционных систем
7	Безопасность систем баз данных
7	Безопасность сетей ЭВМ
9	Защита информации в сенсорных сетях

10.3. В качестве критериев оценки уровня сформированности (освоения) у обучающихся компетенций применяется шкала модульно–рейтинговой системы университета. В таблице 15 представлена 100–балльная и 4-балльная шкалы для оценки сформированности компетенций.

Таблица 15 –Критерии оценки уровня сформированности компетенций

Оценка компетенции		Характеристика сформированных компетенций
100-балльная шкала	4-балльная шкала	
$85 \le К \le 100$	«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.

$70 \le К \le 84$	«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.
$55 \le К \le 69$	«удовлетво-рительно» «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.
$К \le 54$	«неудовлетво-рительно» «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; - не формулирует выводов и обобщений.

10.4. Типовые контрольные задания или иные материалы:

1. Вопросы (задачи) для экзамена (таблица 16)

Таблица 16 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена
1	Предмет и задачи курса.
2	Значение и место курса в, подготовке специалистов, по защите информации
3	Анализ нормативных источников, научной и учебной литературы
4	Становление и развитие понятия "информационная безопасность". Современные подходы к определению понятия.
5	Сущность информационной безопасности. Объекты информационной безопасности
6	Связь информационной безопасности с информатизацией общества
7	Значение информационной, безопасности для субъектов информационных
8	Место информационной, безопасности, в системе национальной безопасности.
9	Существующие подходы к содержательной части понятия "защита информации" и способы реализации содержательной части
10	Понятие уязвимости информации
11	Методологическая основа раскрытия сущности и определения понятия защиты информации.
12	Понятие носитель защищаемой информации". Соотношение между носителем и источником информации.
13	Виды отображения информации в носителях
14	Современные подходы к понятию угрозы защищаемой информации
15	Понятие угрозы защищаемой информации.
16	Понятие объекта защиты.
17	Состав объектов хранения письменных и видовых носителей информации, подлежащих защите.

18	Другие объекты защиты информации. Виды и способы дестабилизирующего воздействия на объекты защиты.
19	Виды защиты информации, сферы их действ
20	Классификация методов защиты информации
21	Понятие и классификация средств защиты информации. Назначение программных, криптографических и технических средств защиты.

2. Вопросы (задачи) для зачета / дифференцированного зачета (таблица 17)

Таблица 17 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифференцированного зачета
	Учебным планом не предусмотрено

3. Темы и задание для выполнения курсовой работы / выполнения курсового проекта (таблица 18)

Таблица 18 – Примерный перечень тем для выполнения курсовой работы / выполнения курсового проекта

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

4. Вопросы для проведения промежуточной аттестации при тестировании (таблица 19)

Таблица 19 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов
	Не предусмотрено

5. Контрольные и практические задачи / задания по дисциплине (таблица 20)

Таблица 20 – Примерный перечень контрольных и практических задач / заданий

№ п/п	Примерный перечень контрольных и практических задач / заданий
1	Структура информационной безопасности. Определение понятия информационная безопасность".
2	Связь между информационной безопасностью и безопасностью информации
3	Понятие и современная концепция национальной безопасности
4	Формы выражения нарушения статуса информации
5	Обусловленность статуса информации ее уязвимостью.
6	Формы проявления уязвимости информации. Виды уязвимости информации
7	Понятие "утечка информации
8	Соотношение форм и видов уязвимости информации
9	Содержательная часть понятия "защита информации
10	Способ реализации содержательной части защиты информации
11	Определение понятия "защита информации", его соотношение с понятием, сформулированным в ГОСТ Р 50922-96
12	Состав носителей защищаемой информации
13	Способы фиксирования информации в носителях
14	Методы воспроизведения отображенной информации в носителях
15	Носители письменной, видовой, излучаемой информации
16	Опосредованные носители защищаемой информации

17	Связь угрозы защищаемой информации с уязвимостью информации. Признаки и составляющие угрозы: явления, факторы, условия.
18	Структура явлений как сущностного выражения угрозы защищаемой информации.
19	Структура факторов, создающих возможность дестабилизирующего воздействия на информацию.
20	Носители информации как конечные объекты защиты
21	Особенности отдельных видов носителей как объектов защиты
22	Состав подлежащих защите технических средств отображения, обработки, хранения, воспроизведения передачи информации.
23	Универсальные методы защиты информации область их применения
24	Области применения организационных, криптографических и инженерно-технических методов защиты информации.

10.5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и / или опыта деятельности, характеризующих этапы формирования компетенций, содержатся в Положениях «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

11. Методические указания для обучающихся по освоению дисциплины

Целью дисциплины является – получение студентами необходимых знаний, умений и навыков в области дискретной математики. Создание поддерживающей образовательной среды преподавания служит участие студентов в конференциях, видеоконференциях, участие в научно-исследовательской работах обучающей кафедры.

Дисциплина предоставляет возможность студентам развить и продемонстрировать навыки в области защиты информации при изучении основных направлений обеспечения информационной безопасности, меры законодательного, административного, процедурного и программно-технического уровней при работе на вычислительной технике и в каналах связи.

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 обучающимся 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;

– научится 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 (Табл.21).

Методические указания для обучающихся по прохождению практических занятий

Практическое занятие является одной из основных форм организации учебного процесса, заключающейся в выполнении обучающимися под руководством преподавателя комплекса учебных заданий с целью усвоения научно-теоретических основ учебной дисциплины, приобретения умений и навыков, опыта творческой деятельности.

Целью практического занятия для обучающегося является привитие обучающемся умений и навыков практической деятельности по изучаемой дисциплине.

Планируемые результаты при освоении обучающемся практических занятий:

– закрепление, углубление, расширение и детализация знаний при решении конкретных задач;

– развитие познавательных способностей, самостоятельности мышления, творческой активности;

– овладение новыми методами и методиками изучения конкретной учебной дисциплины;

– выработка способности логического осмысления полученных знаний для выполнения заданий;

– обеспечение рационального сочетания коллективной и индивидуальной форм обучения.

Функции практических занятий:

– познавательная;
– развивающая;
– воспитательная.

По характеру выполняемых обучающимся заданий по практическим занятиям подразделяются на:

– ознакомительные, проводимые с целью закрепления и конкретизации изученного теоретического материала;

– аналитические, ставящие своей целью получение новой информации на основе формализованных методов;

– творческие, связанные с получением новой информации путем самостоятельно выбранных подходов к решению задач.

Формы организации практических занятий определяются в соответствии со специфическими особенностями учебной дисциплины и целями обучения. Они могут проводиться:

– в интерактивной форме (решение ситуационных задач, занятия по моделированию реальных условий, деловые игры, игровое проектирование, имитационные занятия, выездные занятия в организации (предприятия), деловая учебная игра, ролевая игра, психологический тренинг, кейс, мозговой штурм, групповые дискуссии);

– в не интерактивной форме (выполнение упражнений, решение типовых задач, решение ситуационных задач и другое).

Методика проведения практического занятия может быть различной, при этом важно достижение общей цели дисциплины.

Требования к проведению практических занятий

Вариант задания по каждой задаче при выполнении практических и контрольных заданий обучающийся получает в соответствии с номером в списке группы. Перед решением задачи обучающемуся следует внимательно ознакомиться с условием задачи, с рассмотренными примерами, а также содержанием соответствующих тем лекционного курса. В соответствии с заданием обучающийся должен привести решение с необходимыми вычислениями и пояснениями, получить требуемые результаты, оформить задание для сдачи преподавателю.

Методические указания для обучающихся по прохождению 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 у 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.

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;
- список литературы, предоставленный преподавателем.

Примерный перечень тем для самостоятельного освоения представлен в таблице 21.

Таблица 21 –Примерный перечень тем для самостоятельного изучения

№ п/п	Название темы
1.	Системы управления доступом в Интернет и контроля корпоративной электронной почты
2.	Утечки информации: источники, правовые и технологические аспекты
3.	Утилизация данных: проблемы повторного использования.
4.	Методы защиты от нелегального использования ПО (и др. IT- ресурсов).
5.	Аспекты защиты информации в системах автоматизированного управления технологическими процессами.
6.	Понятие политики безопасности
7.	Эволюция вредоносного ПО (malware) и средств борьбы с ним.
8.	Проблемы противодействия фишингу и фармингу.
9.	P2P-приложения: тенденции развития и аспекты безопасности.
10.	Безопасность Web-браузеров.
11.	Безопасность беспроводных технологий.
12.	Виртуальные частные сети (VPN) – технологии и средства организации.
13.	СПАМ: способы распространения, принципы и средства. Противодействия
14.	Защита персональных данных, типовые решения.
15.	Биометрические системы аутентификации: принципы, технологии и перспективы.
16.	Средства взлома парольных систем и противодействие им.

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.

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».

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программам высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

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