МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

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

Кафедра №2

«УТВЕРЖДАЮ»
Руководитель направления
д.э.н.,доц.
(должность, уч. степень, звание)

А.С. Будагов
(подпись)
«31» августа 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы информационной безопасности»
(Название дисциплины)

Код направления	38.03.01
Наименование направления/ специальности	Экономика
Наименование направленности	Финансы и кредит
Форма обучения	очная

Ивангород 2021

Лист согласования рабочей программы дисциплины

Программу составил(а)

доцент, к.т.н.	31.08.2021	А.В. Дагаев
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Программа одобрена на заседании кафедры № 2

«31» августа 2021 г, протокол № 1/1

Заведующий кафедрой № 2

зав.каф., к.ф-м.н., доцент	31.08.2021	Е.А. Яковлева
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Ответственный за ОП 38.03.01(07)

доц.,к.э.н., доц.	31.08.2021	Н.А. Иванова
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Заместитель директора института (декана факультета) № 1И по методической работе

старший преподаватель	31.08.2021	М.М. Маскатулин
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

Аннотация

Дисциплина «Основы информационной безопасности» входит в базовую часть образовательной программы подготовки обучающихся по направлению 38.03.01 «Экономика» направленность «Финансы и кредит». Дисциплина реализуется кафедрой №2.

Дисциплина нацелена на формирование у выпускника

общекультурных компетенций:

ОК-7 «способность к самоорганизации и самообразованию»;

общепрофессиональных компетенций:

ОПК-1 «способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности».

Содержание дисциплины охватывает круг вопросов, связанных с использованием информационных технологий в профессиональной деятельности, обработкой, хранением и передачей данных, использованием программного обеспечения для реализации производственных задач, поиск и безопасность информации в глобальных вычислительных сетях.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа студента.

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

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

Язык обучения по дисциплине «русский».

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Цели дисциплины:

- Формирование у студентов базовых знаний информационной безопасности;
- Обучение студентов методологиям и теоретическим основам защиты данных;
- Обучение студентов методам и процедурам противодействия информационным угрозам;
- Получение студентами практических навыков в обеспечении информационной безопасности и защите данных.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОК-7 «способностью к самоорганизации и самообразованию»,

знать - Источники и методы поиска информации по данной дисциплине и вопросам

уметь-использовать информацию, полученную из источников и анализировать применять полученные знания в соответствии с задачами дисциплины

владеть навыками - самоорганизации и самообразования

иметь опыт деятельности - самоорганизации и самообразования с использованием информационных технологий

ОПК-1 «способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности»,

знать - Правила и методы решения задача, а так же поиск решения в различных источниках с использованием современных технологий, при соблюдении требования информационной безопасности

уметь- Применять требования информационной безопасность при решении задач профессиональной деятельности, поиске требуемой информации в глобальной вычислительной сети

владеть навыками - решения стандартных задач в профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий

иметь опыт деятельности - по решению задач в профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий

2. Место дисциплины в структуре ОП

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

- Информатика
- Информационные технологии в экономике
- Бухгалтерский учет
- Страхование
- Налоги и налогообложение

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

- Банковское дело
- Международные стандарты учета и финансовой отчетности
- Финансовая среда предпринимательства и предпринимательские риски
- Внутренний аудит финансово-хозяйственной деятельности фирмы

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
		№8
1	2	3
Общая трудоемкость дисциплины, ЗЕ/(час)	3/ 108	3/ 108
Аудиторные занятия, всего час., ***В том числе***	16	16
лекции (Л), (час)	8	8
Практические/семинарские занятия (ПЗ), (час)	8	8
лабораторные работы (ЛР), (час)		
курсовой проект (работа) (КП, КР), (час)		
Экзамен, (час)	9	9
Самостоятельная работа, всего	83	83
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 8					
Тема 1 Классификация угроз информационной безопасности. Развитие Информационного пространства	1	2			
Тема 2 Стандарты информационной безопаности. Законодательная база	1				
Тема 3 Программные и аппаратные средства защиты АИС и БД	1	2			
Тема 4 Безопасность и работа с данными в АИС .	1				
Тема 5 Вредоносное программное обеспечение.	1				
Тема 6 Криптографическая защита данных	1	3			
Тема 7 Защищенные каналы связи	1				
Тема 8 Организационные мероприятия по защите данных	1	2			
Итого в семестре:	8	8			30
Итого:	8	8	0	0	83

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.	Тема 1 Классификация угроз информационной безопасности. Развитие Информационного пространства Виды угроз информационной безопасности. Источники. Объекты защиты ИБ. Информационное пространство и риски роста. Обмен данными.
2.	Тема 2 Стандарты информационной безопаности. Законодательная база. Правовые и регламентирующие документы в области защиты данных. Международные стандарты. Доктрина ИБ.
3.	Тема 3 Программные и аппаратные средства защиты АИС и БД Шредеры. Токены. Ключи. Шлюзы. Программное обеспечение для защиты АИС и БД. Системы СКУД.
4.	Тема 4 Безопасность и работа с данными в АИС. Основы безопасной работы с данными в АИС и БД. Авторизация и аутентификация.

5.	Тема 5 Вредоносное программное обеспечение. Классификация вредоносного ПО. Признаки заражения. Методы противодействия и обнаружения. Профилактика заражения.
6.	Тема 6 Криптографическая защита данных Криптографические основы защиты данных. Алгоритмы шифрования. Методы применяемые в системах для защиты данных
7.	Тема 7 Защищенные каналы связи Технологии сетевой безопасности и передачи данных. Организация удаленного документооборота с использование глобальных вычислительных сетей VIPNET, VPN, HTTPS, SSH
8.	Тема 8 Организационные мероприятия по защите данных Применение стандартов безопасности и правых регламентирующих документов к организации ИБ на предприятии. Роли и политика безопасности работы в АИС. Аудит информационной безопасности.

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)	№ раздела дисципл-лины
Семестр 8				
1.	Анализ информационных рисков и угроз использования ПО	Развернутая беседа Решение практических задач	2	
2.	Анализ ИБ предприятия на основе Стандарта ИБ	Развернутая беседа Решение практических задач	1	
3.	Криптографические методы. Шифр Цезаря	Развернутая беседа Решение практических задач	1	
4.	Криптографические методы. Шифр Плейфера	Развернутая беседа Решение практических задач	1	
5.	Криптографические методы. Виженер	Развернутая беседа Решение практических задач	1	
6.	Создание набора ролей для работы АИС	Развернутая беседа Решение практических задач	1	
7.	Формирование политики безопасности для АИС	Развернутая беседа Решение практических задач	1	
		Всего:	8	

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)	№ раздела дисциплины
Учебным планом не предусмотрено			

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 8, час
1	2	3
Самостоятельная работа, всего	83	83
изучение теоретического материала дисциплины (ТО)	63	63
курсовое проектирование (КП, КР)	-	-
расчетно-графические задания (РГЗ)	-	-
выполнение реферата (Р)	20	20
Подготовка к текущему контролю (ТК)	-	-
домашнее задание (ДЗ)	-	-
контрольные работы заочников (КРЗ)	-	-

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)
	Нестеров С.А. Основы информационной безопасности [Электронный ресурс] : учеб. пособие — Электрон. дан. — Санкт-Петербург : Лань, 2016. — 324 с. — Режим доступа: https://elanbook.com/book/75515. — Загл. с экрана.	
	Е. Баранова, А. Бабаш "Информационная безопасность и защита информации" 3-е изд. - М.: Форум: НИЦ ИНФРА-М, 2016. - 322 с.; 60x90 1/16. https://znanium.com/catalog/product/495249	

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)
681.3 П 18	Информационная безопасность [Текст] : учебное пособие Т. Л. Партыка, И. И. Попов. - М. : ФОРУМ ; [Б. м.] : ИНФРА-М, 2004. - 368 с. : рис. - (Профессиональное образование). - Библиогр.: с. 343 - 344 (29 назв.). - **ISBN** 5-8199-0060-X (ФОРУМ). - **ISBN** 5-16-001155-2 (ИНФРА- М) : 53 р., 57 р	10
004(075) К 92	**Основы защиты информации** [Текст] : учебное пособие / А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. - 2-е изд., стер. - М. : Академия, 2007. - 256 с. : рис. - (Высшее профессиональное образование. Радиоэлектроника). - Библиогр.: с. 251 - 252 (32 назв.). - **ISBN** 978-57695-4416-3 : 200.00 р	10
Х К67	Информационная безопасность предприятия [Текст] : монография / И. Р. Конеев, А. В. Беляев. - СПб. : БХВ - Петербург, 2003. - 752 с. : рис., табл. - Библиогр.: с. 718 - 723. -Предм. указ.: с. 725 - 733. - ISBN 5-94157280-8 : 170.10 р	20
Х	Информационная безопасность [Текст] : учебник / В. И.Ярочкин. - М. : Летописец ; М. : Междунар. отношения,	20

Я76	2000. - 396 с. : схем. - Библиогр.: с. 394 - 396. - ISBN 5-7133-0993-2. - ISBN 5-93186-006-1 : 70.00 р. Издание выпущено в рамках Федеральной программы книгоиздания России. Издание имеет гриф Министерства образования РФ. На с. 256 - 394	
004(075) М21	Информационная безопасность: концептуальные и методологические основы защиты информации [Текст] : учебное пособие / А. А. Малюк. - М. : Горячая линия - Телеком, 2004. - 280 с. : рис. - (Специальность для высших учебных заведений). - Библиогр.: с. 276 - 278 (51 назв.). - ISBN 5- 93517-197-X : 110.70 р	15

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.consultant.ru/	Консультант +
http://www.garant.ru/	Гарант
http://window.edu.ru/	Едино окно доступа к информационным ресурсам
https://www.intuit.ru/studies/courses/10/10/info	Онлайн курс информационной безопасности

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	Microsoft Office Professional Plus 2010/13/16
2	Microsot Windows 7/8/10 Professional
	Договор: №51656 от 17.01.2012
	Договор: №71955/168-7 от 22.03.2017
	Acrobat Reader DC -
3	(https://acrobat.adobe.com/ru/ru/acrobat/pdf-reader/volume-distribution.html)
4	CrypTool 2.0 https: //www.cryptool .org/en/cryptool2

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 ИФГУАП для проведения лекционных и практических (семинарских) занятий	
2	Кабинет информационных технологий и программных систем Проектор BENQ MW526E DLP Ноутбук HP 250 G4 Экран для проектора настенный Lumien Master Picture 244*184 Планшет графический WACOM ONE M Программно аппаратный комплекс ASCOD GARANT Сервер ASCOD-Garant с комплектом рельсов для монтажа ИБП Ippon Smart Winner 2000VA Роутер Mikro Tik RB2011UiAS-RM Персональные компьютеры (17 шт.), орг.техника, локальная сеть с выходом в сеть университета и Интернет	212

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

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
ОК-7 «способность к самоорганизации и самообразованию»	
1	История

1	История экономических учений
1	Иностранный язык
1	Математика. Математический анализ
1	Безопасность жизнедеятельности
1	Физическая культура
1	Информатика
1	Экономика. Микроэкономика
2	Иностранный язык
2	Правоведение
2	Прикладная физическая культура (элективный модуль)
2	Математика. Аналитическая геометрия и линейная алгебра
2	Философия
2	Информатика
2	Экономика. Макроэкономика
2	Математика. Математический анализ
2	Учебная практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности
3	Математика. Теория вероятностей и математическая статистика
3	Социология и политология
3	Статистика
3	Мировая экономика и международные экономические отношения
3	Экономика организации
3	Менеджмент
3	Иностранный язык
3	Прикладная физическая культура (элективный модуль)
4	Маркетинг
4	Психология и педагогика
4	Финансовая математика
4	Математика. Теория вероятностей и математическая статистика
4	Финансы
4	Прикладная физическая культура (элективный модуль)
4	Производственная практика по получению профессиональных умений и опыта профессиональной деятельности
4	Мировая экономика и международные экономические отношения
4	Бухгалтерский учет
4	Иностранный язык
5	Страхование
5	Деловой иностранный язык

5	Финансовый анализ
5	Информационно-аналитическая деятельность на предприятиях
5	Ценообразование
5	Прикладная физическая культура (элективный модуль)
5	Эконометрика
5	Бухгалтерское дело
5	Деньги, кредит, банки
5	Бухгалтерский учет
6	Инвестиции
6	Основы аудита
6	Инвестиции и кредитование
6	Основы информационной безопасности
6	Комплексный экономический анализ финансово-хозяйственной деятельности
6	Прикладная физическая культура (элективный модуль)
6	Налоги и налогообложение
6	Производственная практика научно-исследовательская работа
6	Деловой иностранный язык
6	Информационные технологии в экономике
6	Анализ финансовой отчётности
7	Макроэкономическое планирование и прогнозирование
7	Финансовые инвестиции
7	Налоговые системы зарубежных стран
7	Финансовый менеджмент
7	Стратегия инновационной деятельности
7	Экономика и финансы предприятия
7	Финансовая среда предпринимательства и предпринимательские риски
7	Бухгалтерская финансовая отчетность
7	Финансовая политика
7	Бюджетная система РФ
7	Процедуры и методы контроля деятельности предприятий
7	Информационные системы финансов и бухгалтерского учета
8	Международные стандарты учета и финансовой отчетности
8	Финансы предприятия
8	Налоговое администрирование
8	Экономика реорганизации фирмы
8	Организация и методика проведения налоговых проверок
8	Иностранные инвестиции
8	Учет и анализ банкротств
8	Внутренний аудит финансово-хозяйственной деятельности фирмы
8	Системы контроля финансов

8	Банковское дело
8	Оперативная финансовая работа
8	Производственная преддипломная практика
ОПК-1 «способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности»	
1	Информатика
2	Информатика
2	Учебная практика по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности
3	Статистика
5	Ценообразование
6	Основы информационной безопасности
6	Информационные технологии в экономике
7	Информационные системы финансов и бухгалтерского учета
8	Иностранные инвестиции

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 ≤ 54	«неудовлетворительно» «не зачтено»	- обучающийся не усвоил значительной части программного материала; - допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; - испытывает трудности в практическом применении знаний; - не может аргументировать научные положения; - 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
	1Методы борьбы с фишинговыми атаками. 2.Законодательство о персональных данных. 3.Защита авторских прав. 4.Назначение, функции и типы систем видеозащиты. 5.Как подписывать с помощью ЭЦП электронные документы различных форматов. 6.Обзор угроз и технологий защиты Wi-Fi-сетей. 7.Проблемы внедрения дискового шифрования. 8.Борьба со спамом: основные подходы, классификация, примеры, прогнозы на будущее. 9.Особенности процессов аутентификации в корпоративной среде. 10.Квантовая криптография. 11.Утечки информации: как избежать. Безопасность смартфонов. 12.Безопасность применения пластиковых карт - законодательство и практика. 13. Криптографические алгоритмы 14.Современные угрозы и защита электронной почты. 15.Программные средства анализа локальных сетей на предмет уязвимостей. 16.Безопасность применения платежных систем - законодательство и практика. 17.Аудит программного кода по требованиям безопасности. 18.Антишпионское ПО (antispyware). 19.Обеспечение безопасности Web-сервисов. 20.Защита от внутренних угроз. 21.Технологии RFID. 22.Уничтожение информации на магнитных носителях. 23.Ботнеты - плацдарм современных кибератак. 24.Цифровые водяные знаки в изображениях. 25.Электронный документооборот. Модели нарушителя. 26.Идентификация по голосу. Скрытые возможности. 27.Безопасность океанских портов. 28.Безопасность связи. 29.Безопасность розничной торговли. 30.Банковская безопасность. 31.Информатизация управления транспортной безопасностью. 32.Биопаспорт. 33.Обзор современных платформ архивации данных. 34.Что такое консалтинг в области ИБ.

	35.Бухгалтерская отчетность как источник рассекречивания информации. 36.Управление рисками: обзор употребительных подходов. 37.Категорирование информации и информационных систем. Обеспечение базового уровня информационной безопасности. 38.Распределенные атаки на распределенные системы. 39.Оценка безопасности автоматизированных систем. 40.Windows и Linux: что безопаснее? 41.Функциональная безопасность программных средств. 42.Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств. 43.Информационная безопасность: экономические аспекты. 44. Угрозы в информационной безопасности. 45. Уязвимости в информационной безопасности. 46. Сетевые атаки. Классификация сетевых атак. 48. Межсетевое экранирование. Классификация межсетевых экранов. 49. Формальные модели политик безопасности. Политики управления доступом и 50. информационными потоками в компьютерных системах. 51. Криптографические методы защиты информации в компьютерных сетях. 52. Применение технологии виртуальных частных сетей. 53. Организация антивирусной защиты информации 54. Средства и методы предотвращения и обнаружения вторжений. 55. Анализ безопасности компьютерных сетей с использованием стандартов ИБ

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 воспитание у студентов необходимого уровня культуры в области информационной безопасности, предоставление возможности обучающимся развить и продемонстрировать навыки в области применения методов шифрования, ознакомление студентов с принципами функционирования и построения систем ИБ, формирование у студентов представления о методах и процедурах противодействия информационным угрозам, обучение методологиям и теоретическим основам защиты данных, получение студентами практических навыков в обеспечении информационной безопасности и защите данных.

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 материала по рассматриваемой теме;
- Демонстрация примеров решения конкретных задач;
- Ответы на возникающие вопросы по теме лекции;
- Выдача раздаточного материала с примерами по теме лекции и дискуссия об их особенностях.

Методические указания для обучающихся по прохождению практических занятий

Практическое занятие является одной из основных форм организации учебного процесса. Оно заключается 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 является привитие обучающимся умений и навыков практической деятельности по изучаемой дисциплине.

Планируемые результаты при освоении обучающимся 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:

- интерактивная форма (обсуждение вариантов схем алгоритмов для решения конкретных практических задач);
- не интерактивная форма (выполнение упражнений, решение типовых задач).

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

Требования к проведению практических занятий

На практических занятиях могут применяться следующие формы работы:

- фронтальная - все студенты выполняют одну и ту же работу;

- групповая - одна и та же работа выполняется бригадами из 2-5 человек;
- индивидуальная - каждый студент выполняет индивидуальное задание.

Рекомендуется проведение сквозных практических работ на основе внутрипредметных связей, когда результаты, полученные в одной практической работе, используются при выполнении последующих практических работ по данной дисциплине.

Для повышения эффективности проведения практических занятий рекомендуются:

- разработка тестов входного контроля подготовленности студентов, в том числе автоматизированного, к выполнению работ и заданий;
- разработка дифференцированных заданий с учетом индивидуальных особенностей обучающихся;
-использование в практике преподавания поисковых работ и заданий на проблемной основе;
-применение коллективных и групповых форм работы, максимальное использование индивидуальных форм с целью повышения ответственности каждого студента за самостоятельное выполнение полного объема работ;
-проведение практических и семинарских занятий на повышенном уровне трудности с включением в них заданий, связанных с выбором условий выполнения работы, конкретизацией цели, самостоятельным отбором необходимого оборудования, с выполнением логических заданий, с поиском мировоззренческого и нравственного выбора.
-подбор дополнительных заданий для студентов, работающих в более быстром темпе, для эффективного использования времени, отводимого на занятии и т.д.;
— разработка заданий для автоматизированного тестового контроля подготовленности студентов к занятиям.

В рамках дисциплины используются такие практические занятия, как групповые дискуссии.

Методика подготовки и проведения групповой дискуссии включает в себя несколько этапов.

1. **Выбор темы.** Тема должна быть актуальной для участников дискуссии, социально значимой, связанной с реальной практикой. Она должна содержать проблемные моменты, вызывать интерес у присутствующих, быть для них достаточно знакомой, чтобы они могли компетентно вести ее обсуждение. Тема должна быть выбрана в рамках тематики практического занятия, но обязательно с учетом интересов участников дискуссии.

Формулировка темы должна быть четкой и ясной, по возможности краткой, привлекающей внимание участников, заставляющей задуматься над поставленной проблемой.

2. **Разработка вопросов для обсуждения.** От того как будут поставлены эти вопросы, во многом зависит успех предстоящего разговора. Формулировка вопросов должна включать в себя возможность предъявления различных точек зрения, быть поводом для размышления. В формулировках могут содержаться мнения, которые не являются бесспорными, могут приводиться положения, противоречащие фактам действительности, отличные от общепринятой трактовки.

3. Разработка сценария дискуссии. Сценарий, как правило, включает: вводное слово руководителя (обоснование выбора данной темы, указание на ее актуальность, задачи, стоящие перед участниками дискуссии); вопросы, вынесенные на обсуждение, условия ведения дискуссии; приемы активизации обучаемых; список литературы, необходимой для изучения.

Основные контуры замысла дискуссии доводятся до ее участников заранее. Обучаемые должны за несколько дней до проведения дискуссии знать тему спора, предложенные для обсуждения вопросы, чтобы изучить проблему, прочитать необходимую литературу, проконсультироваться со специалистами, проанализировать различные точки зрения, сопоставить их, определить собственную позицию.

4. **Непосредственное проведение групповой дискуссии на учебном занятии.** Ведущий во вступительном слове напоминает тему, цели и задачи дискуссии, предлагаемые вопросы для обсуждения.

После вводного слова ведущий начинает дискуссию постановкой вопроса или комментариями по проблеме, приглашает присутствующих высказать собственное мнение по первому вопросу. Он предоставляет слово желающим выступить, активно содействует естественному развитию обсуждения, втягивает в активный обмен мнениями всех участников.

Вводная часть — важный и необходимый элемент в любой дискуссии, так как участникам необходим интеллектуальный и эмоциональный настрой на работу, на предстоящее обсуждение. ***Варианты организации вводной части*** могут быть и иные:

— заранее поставить перед одним или двумя участниками задачу выступить с вводным проблемным сообщением, раскрывающим постановку проблемы;
— кратко обсудить вопрос в малых группах;
— использовать краткий опрос по теме.

Любой из вариантов не должен занимать много времени, чтобы можно было быстрее перейти

к дискуссии.

Руководитель может задавать вопросы участникам разговора, ограничивать их, если они выходят за рамки обсуждаемой темы. Он может применять специальные приемы для повышения активности аудитории: подбадривать «противников»; заострять противоположные точки зрения; использовать противоречия, разногласия в суждениях выступающих, обращать доводы спорящего против него самого; предупреждать возможные возражения со стороны спорящих; создавать затруднительные ситуации, когда выдвигаются примеры, содержащие противоречивые моменты, сложные решения, делающие возможным появление различных точек зрения.

При руководстве дискуссией продуктивность выдвижения гипотез и идей повышается, если ведущий:

— дает время на обдумывание ответов;

— избегает неопределенных двусмысленных вопросов;

— обращает внимание на каждый ответ;

— изменяет ход рассуждения участников — расширяет мысль или меняет ее направленность (например, задает вопросы типа: «Какие еще сведения можно использовать? Какие еще факторы могут оказывать влияние? Какие здесь возможны альтернативы?» и т.д.);

— побуждает участников к углублению мысли (например, с помощью вопросов: «Итак, у вас есть ответ? Как вы к нему пришли? Как можно доказать, что это верно?»).

Ведущему следует поощрять участников спора, используя такие реплики, как: «интересная мысль», «хорошая постановка вопроса», «давайте разберемся, подумаем» и т.п. Он должен помогать выступающим в четкой формулировке мыслей, подборе нужных слов. Не нужно уходить от неожиданных вопросов, отказываться от обсуждения частных проблем, ссылаясь на их несоответствие плану дискуссии.

По результатам обсуждения проблемы ведущему необходимо сделать вывод и переходить к следующему вопросу.

5. Разбор, подведение итогов дискуссии. Ведущий подводит итоги дискуссии, анализирует выводы, к которым пришли участники спора, подчеркивает основные моменты правильного понимания проблемы, показывает ложность, ошибочность высказываний, несостоятельность отдельных позиций по конкретным вопросам темы спора. Он обращает внимание на содержание речей, точность выражения мыслей, глубину и научность аргументов, правильность употребления понятий, оценивает умение отвечать на вопросы, применять различные средства полемики, отмечает наиболее активных участников дискуссии, дает рекомендации по дальнейшему изучению обсуждаемой проблемы, совершенствованию полемических навыков и умений.

Иногда, если состав учебной группы велик, ведущий в начале занятия создает дискуссионные группы, в которых и идет первоначальное обсуждение вынесенной для спора проблемы.

Решение практических задач по темам раздела призвано закрепить, углубить, расширить и детализировать знания при решении конкретных жизненных ситуаций, выработать способности логического осмысления полученных знаний для выполнения профессиональных задач, обеспечить рациональное сочетание коллективной и индивидуальной форм обучения. Условия задач в письменной форме предоставляются преподавателем. Вопросы к условию задачи могут меняться.

Методические указания для обучающихся по прохождению самостоятельной работы

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

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

Для обучающихся по заочной форме обучения, самостоятельная работа включает в себя контрольную работу. Перечень заданий, а также методические рекомендации к выполнению контрольных работ находятся на официальном сайте ИФ ГУАП в разделе «Задания»: https://pro.guap.ru

Методическими материалами, направляющими самостоятельную работу обучающихся является учебно-методический материал по дисциплине;

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».

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

Рефератные задания, примерный перечень тем:

1. Теоретические и концептуальные основы защиты информации.
2. Принципы защиты информации.
3. Цели и значение защиты информации.
4. Задачи защиты информации и функции по их реализации.
5. Виды, методы и средства защиты информации.
6. Кадровое и ресурсное обеспечение защиты информации.
7. Источники дестабилизирующего воздействия на информацию.
8. Каналы утечки информации ограниченного доступа.
9. Современные подходы к понятию угрозы защищаемой информации.
10. Объекты защиты информации.
11. Структура системы защиты информации, назначение составных частей системы.
12. Понятие «носитель защищаемой информации». Соотношение между носителем и источником информации.
13. Классификация мероприятий по защите информации, сферы применения организационно-технологических документов и мероприятий.
14. Объекты (предметы) интеллектуальной собственности как составная часть защищаемой информации.
15. Собственники и владельцы информации, отнесенной к служебной и профессиональной тайне.
16. Функции должностных лиц, наделенных полномочиями по отнесению сведений к государственной тайне.
17. Правовые и организационные принципы отнесения информации к защищаемой.
18. Криминалистическая характеристика компьютерной преступности в России.
19. Состав и классификация носителей защищаемой информации.
20. Понятие утечки информации, виды и причины утечки информации.
21. Состав подлежащих защите технических средств отображения, обработки, хранения, воспроизведения и передачи информации.
22. Способы совершения компьютерных преступлений.
23. Модели безопасного подключения к Интернет.
24. Организация противодействия вредоносным программам.
25. Компьютерные преступления, получившие мировую известность.
26. Хакерство.
27. Кардерство, как вид компьютерных преступлений.
28. Проблемы ОВД по расследованию компьютерных преступлений.
29. Государственные органы управления в области информационной безопасности, их права и обязанности.
30. Понятие «информационная война», виды и средства, применяемые в информационной войне.

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