

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

доц., к.т.н., доц.

(должность, уч. степень, звание)

А.А. Овчинников

(инициалы, фамилия)

(подпись)

«19» мая 2021 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Организационное и правовое обеспечение информационной безопасности»
(Наименование дисциплины)

Код направления подготовки/ специальности	10.03.01
Наименование направления подготовки/ специальности	Информационная безопасность
Наименование направленности	Безопасность компьютерных систем
Форма обучения	очная

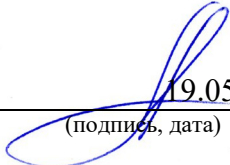
Санкт-Петербург – 2021

Лист согласования рабочей программы дисциплины

Программу составил (а)

зав.каф., к.т.н., доц.

(должность, уч. степень, звание)

 19.05.2021
(подпись, дата)

А.А. Овчинников

(инициалы, фамилия)

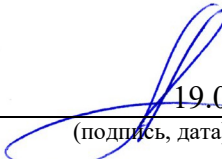
Программа одобрена на заседании кафедры № 51

«19» мая 2021 г, протокол №10

Заведующий кафедрой № 51

к.т.н., доц.

(уч. степень, звание)

 19.05.2021
(подпись, дата)

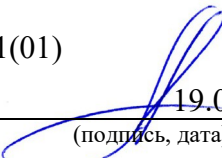
А.А. Овчинников

(инициалы, фамилия)

Ответственный за ОП ВО 10.03.01(01)

доц., к.т.н., доц.

(должность, уч. степень, звание)

 19.05.2021
(подпись, дата)


А.А. Овчинников

(инициалы, фамилия)

Заместитель директора института №5 по методической работе

доц., к.т.н., доц.

(должность, уч. степень, звание)

 19.05.2021
(подпись, дата)

О.И. Красильникова

(инициалы, фамилия)

Аннотация

Дисциплина «Организационное и правовое обеспечение информационной безопасности» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 10.03.01 «Информационная безопасность» направленности «Безопасность компьютерных систем». Дисциплина реализуется кафедрой «№51».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

УК-2 «Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений»

ОПК-5 «Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности»

ОПК-6 «Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю»

ОПК-10 «Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты»

Содержание дисциплины охватывает круг вопросов, связанных с законодательной и административной стороной обеспечения информационной безопасности

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, практические занятия, самостоятельная работа студента.

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

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа.

Язык обучения по дисциплине «русский»

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Цель преподавания дисциплины — формирование единого целостного представления о задаче обеспечения информационной безопасности и путях ее решения применительно к профилю подготовки.

1.2. Дисциплина входит в состав обязательной части образовательной программы высшего образования (далее – ОП ВО).

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

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями или их частями. Компетенции и индикаторы их достижения приведены в таблице 1.

Таблица 1 – Перечень компетенций и индикаторов их достижения

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Универсальные компетенции	УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.3.2 знать действующее законодательство и правовые нормы, регулирующие профессиональную деятельность УК-2.У.2 уметь использовать нормативную и правовую документацию УК-2.В.1 владеть навыками выбора оптимального способа решения задач с учетом действующих правовых норм
Общепрофессиональные компетенции	ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.3.1 знает основы: российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в Российской Федерации ОПК-5.3.2 знает основные понятия и характеристику основных отраслей права применяемых в профессиональной деятельности организации ОПК-5.3.3 знает основы законодательства Российской Федерации, нормативные правовые акты, нормативные и методические документы в области информационной безопасности и защиты информации, правовые основы организации защиты государственной тайны и конфиденциальной информации, правовую характеристику преступлений в сфере компьютерной информации и меры правовой и дисциплинарной ответственности за разглашение защищаемой информации ОПК-5.3.4 знает правовые основы

		<p>организации защиты персональных данных и охраны результатов интеллектуальной деятельности</p> <p>ОПК-5.У.1 умеет обосновывать решения, связанные с реализацией правовых норм по защите информации в пределах должностных обязанностей, предпринимать необходимые меры по восстановлению нарушенных прав</p> <p>ОПК-5.У.2 умеет анализировать и разрабатывать проекты локальных правовых актов, инструкций, регламентов и организационно-распорядительных документов, регламентирующих работу по обеспечению информационной безопасности в организации</p> <p>ОПК-5.У.3 умеет формулировать основные требования при лицензировании деятельности в области защиты информации, сертификации и аттестации по требованиям безопасности информации</p> <p>ОПК-5.У.4 умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации</p>
<p>Общепрофессиональные компетенции</p>	<p>ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и</p>	<p>ОПК-6.3.1 знает систему нормативных правовых актов и стандартов по лицензированию в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации</p> <p>ОПК-6.3.2 знает задачи органов защиты государственной тайны и служб защиты информации на предприятиях</p> <p>ОПК-6.3.3 знает систему организационных мер, направленных на защиту информации ограниченного доступа</p> <p>ОПК-6.3.4 знает нормативные, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации ограниченного доступа</p> <p>ОПК-6.У.4 умеет формулировать основные требования, предъявляемые к физической защите объекта и</p>

	экспортному контролю	пропускному режиму в организации
Общепрофессиональные компетенции	ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.3.2 знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности

2. Место дисциплины в структуре ОП

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

- «Защита и обработка конфиденциальных документов»,
- «Документоведение»,
- «Основы информационной безопасности».

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и используются при выполнении выпускной квалификационной работы.

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
		№8
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	2/ 72	2/ 72
Из них часов практической подготовки		
Аудиторные занятия, всего час.	40	40
в том числе:		
лекции (Л), (час)	20	20
практические/семинарские занятия (ПЗ), (час)	20	20
лабораторные работы (ЛР), (час)		

курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)		
Самостоятельная работа , всего (час)	32	32
Вид промежуточной аттестации: зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.**)	Зачет	Зачет

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 8					
Введение	4	4			4
Раздел 1. Иерархия законов и подзаконных актов по вопросам информационной безопасности					
Раздел 2. Структура службы безопасности предприятия	4	4			4
Раздел 3 Трудовой кодекс.	2	2			4
Раздел 4 Гражданский кодекс.	2	2			4
Раздел 5 Обработка инцидентов безопасности	4	4			4
Раздел 6 Уголовно-процессуальный кодекс	2	2			4
Раздел 7 Правила техники электробезопасности	2	2			4
Заключение					
Текущий контроль					4
Итого в семестре:	20	20			32
Итого	20	20	0	0	32

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	Тема 1.1. Конституция Российской Федерации. Тема 1.2. Доктрины, концепции. Федеральные законы. Подзаконные акты. ФСБ, ФСТЭК, другие федеральные учреждения-регуляторы и их требования. Тема 1.3. Источники информации.
2	Тема 2.1. Задачи основных подразделений службы

	<p>безопасности предприятия, их связь с текущим состоянием предприятия.</p> <p>Тема 2.2. Модель СММ, модели Грейнера и Адизеса.</p> <p>Тема 2.3. Методики планирование работы службы безопасности</p>
3	Тема 3.1. Прием на работу, организация труда и отдыха, права и обязанности сторон, особые обязанности с точки зрения информационной безопасности, их оформление.
4	Тема 4.1. Соблюдение авторских прав. Тема 4.2. Проприетарные и OpenSource программные продукты.
5	Тема 5.1. Жизненный цикл инцидента безопасности. Цикл PDCA (Plan Do Check Act)/ Организация взаимодействия при обработке инцидента безопасности. Тема 5.2. Инсайдеры. Информационная сторона рейдерства. Тема 5.3. Социальная инженерия Тема 5.4. Уязвимости, атаки и защита от них.
6	Тема 6.1. Элементы форензики при расследовании компьютерных преступлений. Тема 6.2. Уголовный процесс. Доказательства, их свойства. Участники, их роли и права. Эксперт.
7	Тема 7.1. Система стандартов безопасности труда. Тема 7.2. Заключение

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
Семестр 8					
1	Структура и активы предприятия	имитационные занятия	2		1
2	Оценка объема трудозатрат. Технические нормативы	решение ситуационных задач	2		2
3	Прием на работу. Резюме. Оформление. Знакомство с предприятием	решение ситуационных задач	2		3
4	Проприетарные и OpenSource программы, их использование.	занятия по моделированию реальных условий	4		4
5	Документация в части информационной безопасности. Документирование инцидентов безопасности.	деловая игра			4
6	Физическая безопасность	занятия по моделированию реальных условий	4		7
Всего			20	0	

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
Учебным планом не предусмотрено				
	Всего			

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 8, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	12	12
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	10	10
Домашнее задание (ДЗ)	10	10
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)		
Всего:	32	32

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)
--------------------	--------------------------	---

Х М 48	Мельников, В. П. Информационная безопасность и защита информации: учебное пособие/В. П. Мельников, С. А. Клейменов, А. М. Петраков; ред. С. А Клейменов. - 5-е изд. стер. - М.: Академия, 2011. - 331 с.	25
Х404.3 М 48	Информационная безопасность и защита информации: учебное пособие/ В. П. Мельников, С. А. Клейменов, А. М. Петраков; ред. С. А Клейменов. - 5-е изд., стер. - М.:Академия, 2011. - 331 с.	25
http://znanium.com/catalog.php?bookinfo=42392	Информационная безопасность компьютер-ных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 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/7/7/info	Тони Хаулет Инструменты безопасности открытым исходным кодом. ИНТУИТ.
http://www.intuit.ru/studies/courses/506/362/info	Борис Позднеев. Стандартизация и сертификация программного обеспечения. ИНТУИТ.
http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-tekhnicheskaya-zashchita-informatsii/dokumenty/spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument	Методический документ. Меры защиты информации в государственных информационных системах. ФСТЭК России, 2014 г.

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
1	http://www.consultant.ru/ Консультант плюс - законодательство Российской Федерации
2	http://www.cntd.ru/ Центр научно-технической документации
3	http://fstec.ru/ портал ФСТЭК

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
Зачет	Список вопросов; Тесты; Задачи.

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

Таблица 14 – Критерии оценки уровня сформированности компетенций

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	
«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;

Оценка компетенции	Характеристика сформированных компетенций
5-балльная шкала	
	– владеет системой специализированных понятий.
«удовлетворительно» «зачтено»	– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; – допускает несущественные ошибки и неточности; – испытывает затруднения в практическом применении знаний направления; – слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий.
«неудовлетворительно» «не зачтено»	– обучающийся не усвоил значительной части программного материала; – допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; – испытывает трудности в практическом применении знаний; – не может аргументировать научные положения; – не формулирует выводов и обобщений.

10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора
	Учебным планом не предусмотрено	

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

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

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета	Код индикатора
1	Иерархия законов и подзаконных актов по вопросам информационной безопасности. Структура и функции федеральных органов исполнительной власти и управления. Указ Президента РФ от 09.03.2004 N 314	УК-2.3.2 УК-2.У.2 УК-2.В.1
2	Конституция Российской Федерации, отражение вопросов информационной безопасности. Соотношение с международными законами	ОПК-5.3.1 ОПК-5.3.2 ОПК-5.3.3 ОПК-5.3.4
3	Доктрины, концепции, Федеральные законы, связанные с вопросами информационной безопасности, их краткое содержание	ОПК-5.У.1 ОПК-5.У.2 ОПК-5.У.3
4	Закон о связи. Обязанности операторов связи. Проведение СОСМ	ОПК-5.У.4 ОПК-6.3.1
5	Подзаконные акты. ФСБ, ФСТЭК, другие федеральные учреждения- регуляторы и их требования.	ОПК-6.3.2 ОПК-6.3.3
6	Структура службы безопасности предприятия. Задачи основных подразделений, их связь с текущим состоянием предприятия.	ОПК-6.3.4 ОПК-6.У.4
7	Модели развития предприятия. Модель СММ, модели	ОПК-10.3.2

8	Грейнера и Адизеса. Задачи службы информационной безопасности на различных этапах развития предприятия. Методики планирования работы службы безопасности. Трудозатраты	
9	Трудовой кодекс. Прием на работу, организация труда и отдыха, права и обязанности сторон, особые обязанности с точки зрения информационной безопасности, их оформление.	
10	Гражданский кодекс. Соблюдение авторских прав, особенности по отношению к программному обеспечению.	
11	Проприетарные и OpenSource программные продукты, особенности лицензий, соблюдение их требований.	
12	Обработка инцидентов безопасности. Жизненный цикл инцидента безопасности.	
13	Порядок служебного расследования инцидентов безопасности	
14	Организация взаимодействия с органами внутренних дел при обработке инцидентов безопасности.	
15	Информационная сторона рейдерства.	
16	Информационные вопросы в законе об оперативно-розыскной деятельности Информационные вопросы в законе о частной детективной и охранной деятельности.	
17	Гражданский кодекс. Соблюдение авторских прав, особенности по отношению к программному обеспечению.	
18	Проприетарные и OpenSource программные продукты, особенности лицензий, соблюдение их требований.	
19	Обработка инцидентов безопасности. Жизненный цикл инцидента безопасности.	
20	Порядок служебного расследования инцидентов безопасности	
21	Организация взаимодействия с органами внутренних дел при обработке инцидентов безопасности.	
22	Информационная сторона рейдерства.	
23	Информационные вопросы в законе об оперативно-розыскной деятельности Информационные вопросы в законе о частной детективной и охранной деятельности	
24	Уголовно-процессуальный кодекс. Уголовный процесс. Участники процесса, их роли и права. Эксперт.	
25	Доказательства, их свойства. Действия эксперта при анализе доказательств.	
26	Модель нарушителя	
27	Элементы форензики при получении доказательств компьютерных преступлений.	
28	Правила техники электробезопасности. ПУЭ.	

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
	Не предусмотрено	

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:

Введение

Раздел 1. Иерархия законов и подзаконных актов по вопросам информационной безопасности

Тема 1.1. Конституция Российской Федерации.

Тема 1.2. Доктрины, концепции. Федеральные законы. Подзаконные акты. ФСБ, ФСТЭК, другие федеральные учреждения-регуляторы и их требования.

Тема 1.3. Источники информации.

Раздел 2. Структура службы безопасности предприятия

Тема 2.1. Задачи основных подразделений службы безопасности предприятия, их связь с текущим состоянием предприятия.

Тема 2.2. Модель СММ, модели Грейнера и Адизеса.

Тема 2.3. Методики планирование работы службы безопасности

Раздел 3. Трудовой кодекс

Тема 3.1. Прием на работу, организация труда и отдыха, права и обязанности сторон, особые обязанности с точки зрения информационной безопасности, их оформление.

Раздел 4. Гражданский кодекс

Тема 4.1. Соблюдение авторских прав.

Тема 4.2. Проприетарные и OpenSource программные продукты.

Раздел 5. Обработка инцидентов безопасности

Тема 5.1. Жизненный цикл инцидента безопасности. Цикл PDCA (Plan Do Check Act)/ Организация взаимодействия при обработке инцидента безопасности.

Тема 5.2. Инсайдеры. Информационная сторона рейдерства.

Тема 5.3. Социальная инженерия

Тема 5.4. Уязвимости, атаки и защита от них.

Раздел 6. Уголовно-процессуальный кодекс

Тема 6.1. Элементы форензики при расследовании компьютерных преступлений.

Тема 6.2. Уголовный процесс. Доказательства, их свойства. Участники, их роли и права. Эксперт.

Раздел 7. Правила техники электробезопасности

Тема 7.1. Система стандартов безопасности труда.

Заключение

11.2. Методические указания для обучающихся по прохождению практических занятий

Практическое занятие является одной из основных форм организации учебного процесса, заключающаяся 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 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.

Требования к проведению практических занятий

Практические занятия проводятся с использованием вычислительных средств.

Преподаватель по окончании практического занятия выдает задание на подготовку к следующему практическому занятию. Этот самостоятельно подготовленный студентами материал используется и развивается на текущем занятии.

Задачи правового обеспечения информационной безопасности решаются для некоторой воображаемой организации, в которой работает обучаемый. Примерный перечень организаций приведен ниже.

1. Главная (Пулковская) астрономическая обсерватория РАН
2. Северо-Западное Управление Федеральной Таможенной Службы
3. ОАО "Кировский завод"
4. Витебский вокзал Санкт-Петербург
5. Морской порт Санкт-Петербург
6. Аэропорт Пулково-2
7. УВД. Управление по борьбе с экономическими преступлениями.
8. Следственный изолятор "Кресты"
9. Мэрия Санкт-Петербурга (Смольный)
10. Балтийский банк. Отделение "Академическое"
11. Санкт-Петербургская антивирусная лаборатория И.Данилова.
12. ЛОМО
13. Интерфакс Северо-Запад Информационное агентство.
14. Управление метрополитена СПб
15. АЭС Сосновый бор
16. Арбитражный суд города Санкт-Петербурга и Ленинградской области
17. НИИ травматологии и ортопедии им.Р.Р.Вредена
18. Сеть гипермаркетов «Лента» - Центральный офис (ул. Савушкина, д. 112)
19. ЦКБ морской техники «Рубин»
20. Фирма «Информационные технологии «ТопПлан»
21. Газета «Аргументы и Факты – Петербург»
22. Военный комиссариат Адмиралтейского и Кировского районов Санкт-Петербурга
23. Районная поликлиника

Чтобы избежать повторений, позиции рекомендуется ежегодно менять
Методические указания по прохождению практических занятий:

Белоголовый В.Г. Методические указания по прохождению практических занятий работ по дисциплине «Организация и правовое обеспечение информационной безопасности». Электронный ресурс кафедры №51.

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 является учебно-методический материал по дисциплине.

Для развития у студентов навыков самостоятельного овладения теоретическим материалом ряд тем дисциплины на лекционных занятиях дается обзорно, что предполагает их самостоятельное детальное изучение.

- Перечень тем для самостоятельного изучения:
- Доктрины, концепции. Федеральные законы. Подзаконные акты. ФСБ, ФСТЭК, другие федеральные учреждения-регуляторы и их требования.
- Модель СММ, модели Грейнера и Адизеса.
- Методики планирование работы службы безопасности
- Прием на работу, организация труда и отдыха, права и обязанности сторон, особые обязанности с точки зрения информационной безопасности, их оформление.
- Соблюдение авторских прав.
- Проприетарные и OpenSource программные продукты.
- Жизненный цикл инцидента безопасности.
- Цикл PDCA (Plan Do Check Act)/ Организация взаимодействия при обработке инцидента безопасности.
- Инсайдеры. Информационная сторона рейдерства.
- Социальная инженерия
- Элементы форензики при расследовании компьютерных преступлений.
- Система стандартов безопасности труда.

11.4. Методические указания для обучающихся по прохождению текущего контроля успеваемости.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины.

Форма проведения текущего контроля – защита отчетов по лабораторным работам. Результаты текущего контроля учитываются при проведении промежуточной аттестации в соответствии с требованиями СТО ГУАП. СМК 3.76 «Положение о текущем контроле успеваемости и промежуточной аттестации студентов и аспирантов ГУАП, обучающихся по образовательным программам высшего образования».

11.5. Методические указания для обучающихся по прохождению промежуточной аттестации.

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

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

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».

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