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
зав. каф., к.т.н., доц.
_____А.А. Овчинников
«15» мая 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Организационное и правовое обеспечение информационной безопасности»

Код направления	10.03.01
Наименование направления/ специальности	Информационная безопасность
Наименование направленности	Комплексная защита объектов информатизации
Форма обучения	очная

Санкт-Петербург 2019 г.

Лист согласования рабочей программы дисциплины

Программу составил

доц., к.т.н. доц. _____ 15.05.2019 В.Г. Белоголовый

подпись, дата

Программа одобрена на заседании кафедры № 51

«15» мая 2019 г., протокол №10

Заведующий кафедрой № 51

доц., к.т.н., доц. _____ 15.05.2019 А.А. Овчинников

подпись, дата

Ответственный за ОП 10.03.01(03)

доц., к.т.н., доц. _____ 15.05.2019 А.А. Овчинников

подпись, дата

Заместитель директора института (факультета) № 5 по методической работе

доц., к.т.н., доц. _____ 15.05.2019 О.И. Красильникова

подпись, дата

Аннотация

Дисциплина «Организационное и правовое обеспечение информационной безопасности» входит в базовую часть образовательной программы подготовки обучающихся по направлению «10.03.01 «Информационная безопасность» направленность «Комплексная защита объектов информатизации». Дисциплина реализуется кафедрой №51.

Дисциплина нацелена на формирование у выпускника

общепрофессиональных компетенций:

ОПК-5 «способность использовать нормативные правовые акты в профессиональной деятельности»;

профессиональных компетенций:

ПК-8 «способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов»,

ПК-15 «способность организовать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю».

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 3 зачетных единицы, 108 часов.

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

В результате освоения дисциплины обучающийся должен обладать следующими компетенциями:

ОПК-5 «способность использовать нормативные правовые акты в профессиональной деятельности»:

знать – действующие нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;

уметь – формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности;

владеть навыками – организации и поддержки выполнения комплекса мер по информационной безопасности, управления процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;

иметь опыт деятельности – в разработке подсистемы управления информационной безопасностью;

ПК-8 «способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов»:

знать – стандарты в области информационной безопасности;

уметь – проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

владеть навыками – анализа информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

иметь опыт деятельности – сборе и проведении анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности;

ПК-15 «способность организовать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю»:

знать − нормативные правовые акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

уметь − организовать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

владеть навыками − применения нормативных правовых актов и нормативных методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в организации процесса защиты информации;

иметь опыт деятельности – в реализации методов защиты информации ограниченного доступа на практике.

2. Место дисциплины в структуре ОП

Дисциплина базируется 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 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
			№
1		2	3
Общая трудоемкость дисциплины,	ЗЕ/(час)	3/ 108	3/ 108
Аудиторные занятия, всего час., ***В том числе***		40	40
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)	68	68
Вид промежуточной аттестации: зачет, экзамен, дифференцированный зачет **(Зачет. Экз. Дифф. зач)**		Зачет	Зачет

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					
Введение Раздел 1. Иерархия законов и подзаконных актов по вопросам информационной безопасности	4	4			4
Раздел 2. Структура службы безопасности предприятия	4	4			8
Раздел 3 Трудовой кодекс.	2	2			10
Раздел 4 Гражданский кодекс.	2	2			10
Раздел 5 Обработка инцидентов безопасности	4	4			8

безопасности					
Раздел 6 Уголовно-процессуальный кодекс	2	2			10
Раздел 7 Правила техники электробезопасности Заключение	2	2			10
Текущий контроль					8
Итого в семестре:	20	20			68
Итого:	20	20	0	0	68

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 1.1. 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 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
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 4.

Таблица 4 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	№ раздела дисциплины
Семестр 8				
1	Структура и активы предприятия	имитационные занятия	2	1
2	Оценка объема	решение	2	2

	трудозатрат. Технические нормативы	ситуационных задач		
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	

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	68	68
Изучение теоретического материала дисциплины (ТО)	40	40
Подготовка к текущему контролю (ТК)	8	8
Домашнее задание (ДЗ)	20	20

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)
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

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)
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
	Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с. http://znanium.com/catalog.php?bookinfo=42392	

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	Наименовани
http://www.intuit.ru/studies/courses/7/7/info	Тони Хаулет Инструменты безопасности с 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, 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
	Не предусмотрено

8.2. Перечень информационно-справочных систем

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11 – Перечень информационно-справочных систем

№ п/п	Наименовани
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, 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	Лекционная аудитория	
2	Лаборатория вычислительной техники	

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
Зачет	Список вопросов.

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-5 «способность использовать нормативные правовые акты в профессиональной деятельности»	
4	Правоведение
8	Организационное и правовое обеспечение информационной безопасности
ПК-8 «способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов»	
2	Учебная практика
3	Документоведение
4	Защита и обработка конфиденциальных документов
6	Мультимедиа технологии

6	Методы и средства обработки изображений
6	Производственная (проектно-технологическая) практика
8	Организационное и правовое обеспечение информационной безопасности
ПК-15 «способность организовать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю»	
4	Технологии программирования
4	Методы и средства защиты информации
4	Производственная практика
5	Цифровая обработка сигналов
5	Технологии программирования
6	Базы данных
7	Базы данных
8	Защита сетей от несанкционированного доступа
8	Организационное и правовое обеспечение информационной безопасности
8	Администрирование в инфокоммуникационных системах

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.
$К \leq 54$	«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
	Учебным планом не предусмотрено

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
	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 2. Конституция Российской Федерации, отражение вопросов информационной безопасности. Соотношение с международными законами 3. Доктрины, концепции, Федеральные законы. связанные с вопросами информационной безопасности, их краткое содержание 4. Закон о связи. Обязанности операторов связи. Проведение СОРМ 5. Подзаконные акты. ФСБ, ФСТЭК, другие федеральные учреждения-регуляторы и их требования. 6. Структура службы безопасности предприятия. Задачи основных подразделений, их связь с текущим состоянием предприятия. 7. Модели развития предприятия. Модель СММ, модели Грейнера и Адизеса. Задачи службы информационной безопасности на различных этапах развития предприятия. 8. 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 17. Информационные вопросы в законе о частной детективной и охранной деятельности

	18. Уголовно-процессуальный кодекс. Уголовный процесс. Участники процесса, их роли и права. Эксперт. 19.Доказательства, их свойства. Действия эксперта при анализе доказательств. 20. Модель нарушителя 21. Элементы форензики при получении доказательств компьютерных преступлений. 22. Правила техники электробезопасности. ПУЭ.

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
	Не предусмотрено

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 единого целостного представления о задаче обеспечения информационной безопасности и путях ее решения применительно к профилю подготовки.

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.

Планируемы 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 пол

– 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 CMM, 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.

Тема 7.2. Заключение

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 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

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.

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.

Методическими материалами, направляющими самостоятельную работу обучающихся являются 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.

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