Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский университет Государственной противопожарной службы МЧС России»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Магистратура по направлению подготовки 27.04.03 «Системный анализ и управление» направление (профиль) «Системный анализ и управление в организационно-технических системах»

Санкт-Петербург

1. Цели и задачи дисциплины

Цели освоения дисциплины:

- формирование у обучающихся целостной системы знаний в области информационной безопасности как фундаментальной базы информационной культуры высокообразованной личности;
- формирование у обучающихся практических навыков по защите информации, необходимых для формирования и развития ряда профессионально важных качеств.

Перечень компетенций, формируемых в процессе изучения дисциплины «Информационная безопасность и защита информации»

Компетенции	Содержание
ПК-5	способен применять методы математического и системного анализа и теории принятия решений для исследования функциональных задач управления организационно-техническими системами на основе отечественных и мировых тенденций развития методов, управления, информационных и интеллектуальных технологий

Задачи дисциплины:

- сформировать знание структуры и основных положения нормативной базы РФ и национальных стандартов в области информационной безопасности и защиты информации, основных каналы реализации угроз безопасности информации, базовых методов и средства защиты информации от несанкционированного доступа;
- сформировать умение идентифицировать основные угрозы безопасности современной ИТ-инфраструктуры, создавать защищенные учетные записи и электронные документы;

– сформировать навыки криптоанализа, владение профессиональной терминологией в сфере информационной безопасности и защиты информации.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
Категория (группа) общепрофессиональных компетенций: управление системами	
Знает способы и методы защиты информации ПК– 5.1	Знает
	структуру и основные положения нормативной базы РФ и национальных стандартов в области информационной безопасности и защиты информации, основных каналы реализации угроз безопасности информации, базовых методов и средства защиты инфор-

	мации от несанкционированного доступа – ПК-5.1
	Умеет
	идентифицировать основные угрозы безопасности современной ИТ-инфраструктуры, создавать защищенные учетные записи и электронные документы – ПК-5.1

3. Место дисциплины в структуре ОПОП

Дисциплина «Информационная безопасность и защита информации» относится к части, формируемой участниками образовательных отношений основной профессиональной образовательной программы магистратуры по направлению подготовки 27.04.03 «Системный анализ и управление», (профиль) «Системный анализ и управление в организационно-технических системах».

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетные единицы: 72 часа.

4.1. Распределение трудоемкости учебной дисциплины по заочной форме обучения и видам работ

Вид учебной работы	Трудоемкость			
	з.е.	час.	по курсам	
			2	3
Общая трудоемкость дисциплины по учебному плану	**2**	**72**	**36**	**36**
Контактная работа, в том числе:		**10**	**2**	**8**
Аудиторные занятия		**10**	**2**	**8**
Лекции (Л)		4	2	2
Практические занятия (ПЗ)		6		6
Самостоятельная работа (СРС)		**62**	**34**	**28**
Зачет с оценкой		**+**		**+**

4.2. **Тематический план, структурированный по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий для заочной формы обучения**

№ п/п	Наименование разделов и тем	Всего часов	Количество часов по видам занятий, в том числе практическая подготовка			Консультация	Контроль	Самостоятельная работа, в том числе консультация
			Лекции	Практические занятия	Лабораторные работы			
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Раздел 1. Понятийный и методологический аппарат, нормативная база и стандарты в области информационной безопасности и защиты информации								
1.	Тема 1. Понятийный и методологический аппарат	10	2					8
2.	Тема 2. Нормативная база и стандарты в области информационной безопасности и защиты информации	8						8
Раздел 2. Каналы реализации угроз безопасности информации								
3.	Тема 3. Каналы силового деструктивного воздействия на информацию	8						8
4.	Тема 4. Технические каналы утечки информации	10						10
5.	**Итого за 1 курс**	**36**	**2**					**34**
6.	Тема 5. Нетрадиционные информационные каналы	12	2	4				6
Раздел 3. Методы и средства защиты информации от несанкционированного доступа								
7.	Тема 6. Криптографическая защита информации	6						6
8.	Тема 7. Методы и средства разграничения и контроля доступа к информации	8		2/2**				6
Раздел 4. Компьютерная преступность, ответственность за нарушения и преступления в сфере информационной безопасности								
9.	Тема 8. Компьютерная преступность. Ответственность за нарушения и преступления в сфере информационной безопасности	10						10

10.	Зачет с оценкой	+					+	
11.	**Итого за 2 курс**	**36**	**2**	**6/2****				**28**
Итого по курсу		**72**	**4**	**6/2****				**62**

4.3 Содержание дисциплины для обучающихся: для заочной формы обучения

РАЗДЕЛ 1. ПОНЯТИЙНЫЙ И МЕТОДОЛОГИЧЕСКИЙ АППАРАТ, НОРМАТИВНАЯ БАЗА И СТАНДАРТЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

Тема 1. Понятийный и методологический аппарат

Лекция. Основные термины и определения в сфере информационной безопасности и защиты информации. «Ландшафт» информационной безопасности: взаимодействие базовых элементов теории. Принципы обеспечения информационной безопасности. Абстрактная модель системы защиты информации: основные понятия. Основы формальной теории защиты информации.

Самостоятельная работа. Модели дискреционного доступа. Модели мандатного доступа. Ролевые модели доступа. Модели безопасности информационных потоков.

Рекомендуемая литература:

основная: [1, 2]

дополнительная: [1]

Тема 2. Нормативная база и стандарты в области информационной безопасности и защиты информации

Самостоятельная работа. Государственная политика в сфере информационной безопасности и защиты информации. Основные нормативные документы, регулирующие отношения в сфере информационной безопасности. Правовые основания отнесения сведений к информации ограниченного доступа. Система защиты государственной тайны в РФ.

Краткая история защиты информации в России. Институт «тайны» в Российском законодательстве. Акты регуляторов в сфере защиты информации. Стандарты в области информационной безопасности и защиты информации.

Рекомендуемая литература:

основная: [1, 2]

дополнительная: [1]

РАЗДЕЛ 2. КАНАЛЫ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Тема 3. Каналы силового деструктивного воздействия на информацию

Самостоятельная работа. Канал силового деструктивного воздействия (СДВ) на информацию по сети электропитания. Канал СДВ по проводным линиям. Канал СДВ по «эфиру». Классификация средств СДВ.

Электромагнитный спектр как источник воздействия на информацию.

Рекомендуемая литература:

основная: [1, 2]

дополнительная: [1]

Тема 4. Технические каналы утечки информации

Самостоятельная работа. Классификация технических каналов утечки информации. Модель и способы утечки по каналу ПЭМИН. Модель и способы утечки по радиоканалу. Модель и способы утечки по электрическому каналу. Модель и способы утечки по акустическому (виброакустическому, акустоэлектрическому) каналу. Модель и способы утечки по ВЧ-каналу. Модель и способы утечки по оптическому (оптико-электронному) каналу.

Электронные устройства негласного получения информации: «жучки», записывающие устройства, подслушивающие устройства. Ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации

Рекомендуемая литература:

основная: [1, 2]

дополнительная: [1]

Тема 5. Нетрадиционные информационные каналы

Лекция. Понятие и обобщенная модель нетрадиционного информационного канала. Методы сокрытия информации в текстовых файлах. Методы сокрытия информации в графических файлах. Методы сокрытия информации в звуковых файлах.

Практическое занятие. Сокрытие информации в тексте.

Самостоятельная работа. Методы сокрытия информации в сетевых пакетах и исполняемых файлах.

Рекомендуемая литература:

основная: [1, 2]

дополнительная: [1,3,4]

РАЗДЕЛ 3. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Тема 6. Криптографическая защита информации

Самостоятельная работа. Модель криптосистемы. Историография и классификация шифров. Примеры криптографических алгоритмов. Криптосистема с симметричными и несимметричными ключами.

Криптоанализ шифров перестановки и простой замены.

Электронная цифровая подпись.

Рекомендуемая литература:

основная: [1, 2]

дополнительная: [1, 2]

Тема 7. Методы и средства разграничения и контроля доступа к информации

Практическая подготовка. Процедура идентификации, аутентификации и авторизации. Система контроля и управления доступом. Система паролирования.

Система охраны периметра.

Рекомендуемая литература:

основная: [1, 2]

дополнительная: [1]

РАЗДЕЛ 4. КОМПЬЮТЕРНАЯ ПРЕСТУПНОСТЬ, ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ И ПРЕСТУПЛЕНИЯ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 8. Компьютерная преступность. Ответственность за нарушения и преступления в сфере информационной безопасности

Самостоятельная работа. Понятие компьютерной преступности. Масштабы и общественная опасность компьютерной преступности. Виды и субъекты компьютерных преступлений. Дисциплинарная ответственность за разглашение охраняемой законом тайны. Административная ответственность за нарушения в сфере информационной безопасности и защиты информации. Уголовная ответственность за преступления в сфере компьютерной информации.

Классификация компьютерных преступлений.

Специфика расследования компьютерных преступлений. Кодификатор Интерпола.

Рекомендуемая литература:

основная: [1, 2]

дополнительная: [1]

5. Методические рекомендации по организации изучения дисциплины

При реализации программы дисциплины используются лекционные и практические занятия.

Общими целями занятий являются:

– обобщение, систематизация, углубление, закрепление теоретических знаний по конкретным темам дисциплины;

– формирование умений применять полученные знания на практике, реализация единства интеллектуальной и практической деятельности;

– выработка при решении поставленных задач профессионально значимых качеств: самостоятельности, ответственности, точности, творческой инициативы.

Целями лекции являются:

– дать систематизированные научные знания по дисциплине, акцентировав внимание на наиболее сложных вопросах;

– стимулировать активную познавательную деятельность обучающихся, способствовать формированию их творческого мышления.

В ходе практического занятия обеспечивается процесс активного взаимодействия обучающихся с преподавателем; приобретаются практические навыки и умения. Цель практического занятия: углубить и закрепить знания, полученные на лекции, формирование навыков использования знаний для решения практических задач; выполнение тестовых заданий по проверке полученных знаний и умений.

Самостоятельная работа обучающихся направлена на углубление и закрепление знаний, полученных на лекциях и других занятиях, выработку навыков самостоятельного активного приобретения новых, дополнительных знаний, подготовку к предстоящим занятиям.

6. Оценочные материалы по дисциплине

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины, проводится в соответствии с содержанием дисциплины по видам занятий в форме тестирования.

Промежуточная аттестация обеспечивает оценивание промежуточных и окончательных результатов обучения по дисциплине, проводится в форме зачета с оценкой.

6.1. Примерные оценочные материалы:

6.1.1. Текущего контроля

Типовые вопросы для опроса

1. Назовите основные стандарты в области информационной безопасности и защиты информации
2. Перечислите и дайте определение основным моделям доступа

3. Перечислите элементы структуры системы защиты государственной тайны

4. Назовите регуляторов в сфере защиты государственной тайны и зоны их ответственности

5. Перечислите порядок допуска должностных лиц и граждан к государственной тайне

6. Назовите типы каналов силового деструктивного воздействия на информационную систему;

7. Перечислите пути проникновения всплеска энергии для каждого из типов каналов силового деструктивного воздействия

8. Приведите классификацию технических каналов утечки информации

9. Дайте определение нетрадиционного информационного канала

10. Приведите классификацию компьютерных преступлений

Типовые задания для тестирования

1. Угроза информационной безопасности – это...
2. Уязвимость – это...
3. Какой степени секретности НЕ существует?
4. Основанием для отказа должностному лицу или гражданину в допуске к государственной тайне могут являться...
5. К органам защиты государственной тайны относятся...
6. Государственную тайну составляют сведения...
7. Условием прекращения допуска к государственной тайне является...
8. Резонирующий емкостной накопитель подключили ко вторичной обмотке трансформаторной подстанции. Определите КСДВ.
9. Мощный разряд молнии в непосредственной близости. Определите КСДВ.
10. Внедрение программной закладки в источник бесперебойного питания. Определите КСДВ.
11. Наводки информационных сигналов в посторонних проводниках (фидерах). Выберите тип ТКУИ.
12. Перехват речевых сигналов направленными микрофонами. Выберите тип ТКУИ.
13. Приём информации, передаваемой закладными устройствами по электросети 220 В. Выберите тип ТКУИ.
14. Беспроводной прием информации, передаваемой закладными устройствами. Выберите тип ТКУИ.
15. Сколько страниц текстовой информации (2000 символов/страница) может быть сокрыто методами стеганографии в мегапиксельной фотографии формата bmp?
16. Сколько страниц текстовой информации может быть сокрыто методами стеганографии в 30 секундах монозвучания файла формата wav?

17. Сколько страниц текстовой информации может быть сокрыто методами стеганографии в 30 секундах стереозвучания файла формата wav?

18. Сколько страниц текстовой информации может быть сокрыто методами стеганографии в 1 странице текстового файла?

19. Как размер криптограммы влияет на успешность и время дешифровки?

20. Сообщение какого объема можно зашифровать, используя «Решетку Кардано» с 15 прорезями для букв?

21. Сообщение какого максимального объема можно зашифровать, используя «Решетку Кардано» 10х10?

22. Компьютерная программа, использующая уязвимости в программном обеспечении и применяемая для проведения атаки на компьютерную систему – это...

23. Дефект алгоритма, который намеренно встраивается в него разработчиком и позволяет получить несанкционированный доступ к данным или удаленному управлению операционной системой и компьютером в целом – это...

24. Ситуация, в которой один человек или программа успешно маскируется под другую путём фальсификации данных, что позволяет получить несанкционированный доступ к данным или удаленному управлению операционной системой и компьютером в целом – это...

6.1.2. Промежуточной аттестации

Примерный перечень вопросов, выносимых на зачет с оценкой

1. Государственная политика в сфере информационной безопасности и защиты информации.
2. Правовое обеспечение информационной безопасности.
3. Конституция РФ об «информационных правах и обязанностях».
4. Основные нормативные документы, регулирующие отношения в сфере информационной безопасности.
5. Акты регуляторов в сфере защиты информации.
6. Институт «тайны» в Российском законодательстве.
7. Классификация тайн.
8. Правовые основания отнесения сведений к категории ограниченного доступа.
9. Краткая история защиты информации в России.
10. Обобщенная модель информационной безопасности.
11. Институт стандартизации сферы информационной безопасности.
12. Национальные стандарты в области информационной безопасности и защиты информации.
13. Международные стандарты в области информационной безопасности и защиты информации.

14. Проблемы гармонизации стандартов информационной безопасности.
15. «Ландшафт» стандартов информационной безопасности.
16. Электромагнитный спектр как источник воздействия на информацию.
17. Каналы силового деструктивного воздействия (СДВ) на информацию.
18. Классификация средств СДВ.
19. Рекомендации по защите компьютерных систем от СДВ.
20. Классификация технических каналов утечки информации.
21. Модель и способы утечки по радиоканалу.
22. Модель и способы утечки по электрическому каналу.
23. Модель и способы утечки по акустическому (вибрационному, акустоэлектрическому) каналу.
24. Модель и способы утечки по параметрическому (смешанному) каналу.
25. Модель и способы утечки по оптическому (оптико-электронному) каналу.
26. Модель и способы утечки по каналу ПЭМИН.
27. Классификация угроз несанкционированного доступа (НСД) к информации.
28. Категории нарушителей безопасности информации и их возможности.
29. Общая характеристика уязвимостей.
30. Способы реализации угрозы НСД к информации.
31. Понятие и обобщенная модель нетрадиционного информационного канала.
32. Методы сокрытия информации в текстовых файлах.
33. Методы сокрытия информации в графических файлах.
34. Методы сокрытия информации в звуковых файлах.
35. Методы сокрытия информации в сетевых пакетах и исполняемых файлах.
36. Модель криптосистемы.
37. Историография и классификация шифров.
38. Примеры криптографических алгоритмов.
39. Криптосистема с симметричными и несимметричными ключами.
40. Электронная цифровая подпись.
41. Мандатная и дискреционная модели доступа.
42. Процедура идентификации, аутентификации и авторизации.
43. Система паролирования.
44. Системы контроля и управления доступом.
45. Система охраны периметра.
46. Современные технологии предотвращения утечки конфиденциальной информации из корпоративной сети.

47. Понятие и функционал DLP-систем.
48. Объем и структура данных защищаемых DLP-системами.
49. Каналы коммуникаций, контролируемые DLP-системами.
50. Критерии оценки программных продуктов, реализующих функциональность DLP.
51. Понятие компьютерной преступности.
52. Масштабы и общественная опасность компьютерной преступности.
53. Виды и субъекты компьютерных преступлений.
54. Специфика расследования компьютерных преступлений.
55. Предупреждение компьютерных преступлений.
56. Кодификатор Интерпола.
57. Дисциплинарная ответственность за разглашение охраняемой законом тайны.
58. Административная ответственность за нарушения в сфере информационной безопасности и защиты информации.
59. Уголовная ответственность за преступления в сфере компьютерной информации.
60. Уголовная ответственность за нарушение закона о государственной тайне.

6.2. Шкала оценивания результатов промежуточной аттестации и критерии выставления оценок

Система оценивания включает:

Форма контроля	Показатели оценивания	Критерии выставления оценок	Шкала оценивания
Зачет с оценкой	правильность и полнота ответа	дан правильный, полный ответ на поставленный вопрос, показана совокупность осознанных знаний по дисциплине, доказательно раскрыты основные положения вопросов; могут быть допущены недочеты, исправленные самостоятельно в процессе ответа.	отлично
		дан правильный, недостаточно полный ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи; могут быть допущены недочеты, исправленные с помощью преподавателя.	хорошо
		дан недостаточно правильный и полный ответ; логика и последовательность изложения имеют	удовлетворительно

		нарушения; в ответе отсутствуют выводы.	
		ответ представляет собой разрозненные знания с существенными ошибками по вопросу; присутствуют фрагментарность, нелогичность изложения; дополнительные и уточняющие вопросы не приводят к коррекции ответа на вопрос.	неудовлетворительно

7. Ресурсное обеспечение дисциплины «Информационная безопасность и защита информации»

7.1. Лицензионное и свободно распространяемое программное обеспечение

Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:

Microsoft Windows 7 Professional – ПО-BE8-834 [Лицензионное]

Microsoft Office Standard 2010 – ПО-413-406 [Лицензионное]

7-Zip – ПО-F33-948 [Свободно распространяемое]

Adobe Acrobat Reader – ПО-F63-948 [Свободно распространяемое]

Google Chrome – ПО-F2C-926 [Свободно распространяемое]

МойОфис Образование – ПО-41B-124 [Свободно распространяемое - Отечественное]

7.2. Профессиональные базы данных и информационные справочные системы

1. Справочная правовая система "КонсультантПлюс: Студент". Режим доступа: http://student.consultant.ru/.

2. Информационно-правовая система «Гарант». Режим доступа: http://www.garant.ru/.

3. Электронная библиотека Санкт-Петербургского университета ГПС МЧС России, обеспечивающая индивидуальный неограниченный доступ из любой точки, в которой имеется доступ к сети Интернет: http://elib.igps.ru.

4. Электронно-библиотечная система IPRbooks, обеспечивающая индивидуальный неограниченный доступ из любой точки, в которой имеется доступ к сети Интернет http://www.iprbookshop.ru.

5. Электронно-библиотечная система «Лань», обеспечивающая индивидуальный неограниченный доступ из любой точки, в которой имеется доступ к сети Интернет https://e.lanbook.com.

7.3. Литература

Основная литература:

1. Безопасность информационных систем и защита информации в МЧС

России: учебное пособие: [гриф МЧС] / Ю.И. Синещук [и др.]; ред. В.С. Артамонов; С.-Петерб. гос. ун-т гос. противопож. службы МЧС России. – СПб.: СПбУ ГПС МЧС России, 2012. –300 с. Режим доступа: http://elib.igps.ru/?4&type=card&cid=ALSFR-6d86bbe6-aeac-49db-bc2e-068c7a55cb8d&remote=false

2. Синещук, Ю.И. Информационные технологии и защита информации в автоматизированных системах управления МЧС России: учебное пособие для слушателей: [гриф МЧС] / Ю.И. Синещук, С.Н. Терехин, В.В. Духанин; ред. В.С. Артамонов; МЧС России. – СПб.: СПбУ ГПС МЧС России, 2010. – 284 с. – Режим доступа: http://elib.igps.ru/?6&type=card&cid=ALSFR-a2e62800-d42d-4e9c-9bc9-4c1d7b9f0f55&remote=false

Дополнительная литература:

1. Проектирование информационных систем [Электронный ресурс]: учебное пособие / С. Ю. Золотов. – Электрон. текстовые данные. – Томск: Томский государственный университет систем управления и радиоэлектроники, Эль Контент, 2013. – 88 с. – 978-5-4332-0083-8. – Режим доступа: http://www.iprbookshop.ru/13965.html

2. Меры защиты информации на уровне пользователя информационно-технологическими средствами: методические указания к самостоятельной работе студентов. Учебно-методическое пособие / Б. А. Бурняшов. – Саратов: Вузовское образование, 2014. – 55 с. – ISBN 2227-8397. http://www.iprbookshop.ru/23077.html

3. Буйневич, М.В. Основы кибербезопасности: способы анализа программ: учебное пособие для студентов высших учебных заведений, обучающихся по УГСН 10.00.00 "Информационная безопасность" по программам подготовки бакалавров, магистров, специалистов для слушателей: [гриф УМО] / М.В. Буйневич, К.Е. Израилов; МЧС России. – СПб.: СПбУ ГПС МЧС России, 2022. – 91 с. – ISBN 978-5-907489-42-4. Режим доступа: http://elib.igps.ru/?8&type=card&cid=ALSFR-00f64c85-4b2e-4cd4-bf09-6434a9411854&query=%D0%91%D1%83%D0%B9%D0%BD%D0%B5%D0%B2%D0%B8%D1%87&remote=false

4. Буйневич, М.В. Основы кибербезопасности: способы защиты от анализа программ: учебное пособие для студентов высших учебных заведений, обучающихся по УГСН 10.00.00 "Информационная безопасность" по программам подготовки бакалавров, магистров, специалистов для слушателей: [гриф УМО] / М.В. Буйневич, К.Е. Израилов; МЧС России. – СПб.: СПбУ ГПС МЧС России, 2022. – 75 с. – ISBN 978-5-907489-43-1. Режим доступа: http://elib.igps.ru/?9&type=card&cid=ALSFR-ff242138-7995-495d-901a-655aaafa7265&query=%D0%91%D1%83%D0%B9%D0%BD%D0%B5%D0%B2%D0%B8%D1%87&remote=false

7.4 Материально-техническое обеспечение дисциплины

Для проведения и обеспечения занятий используются помещения, которые представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой магистратуры, оснащенные оборудованием и техническими средствами обучения: автоматизированное рабочее место преподавателя, маркерная доска, мультимедийный проектор, документ-камера, посадочные места обучающихся.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде университета.

Автор: д.т.н., профессор Буйневич М.В.