ФГБОУ ВО «Санкт-Петербургский университет ГПС МЧС России»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ И ЗАЩИТА ИНФОРМАЦИИ

Специалитет по специальности
27.05.01 Специальные организационно-технические системы

специализация «Информационно-аналитическая деятельность в специальных организационно-технических системах»

Санкт-Петербург

1. Цель 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 «Безопасность информационных систем и защита информации»

Компетенции	Содержание
ПК-3	Способен применять технологии информационно-аналитической деятельности в специальных организационно-технических системах для решения задач поддержки принятия решений в области предупреждения и ликвидации ЧС.

Задачи дисциплины:

– сформировать знание структуры и основных положений системы защиты государственной тайны;

– сформировать знание основных каналов реализации угроз безопасности информации;

– сформировать знание базовых методов и средств защиты информации от несанкционированного доступа;

– сформировать знание современного состояния компьютерной преступности и ответственности за нарушения и преступления в сфере информационной безопасности.

– умение ориентироваться в нормативно-правовой базе и стандартах в области информационной безопасности и защиты информации;

– умение идентифицировать основные угрозы безопасности современных информационных систем;

– умение создавать защищенные учетные записи и защищать электронные документы;

– умение классифицировать компьютерные преступления.

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

Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ПК-3.1 Использует принципы построения информационных систем, методов обработки больших данных, особенности построения интеллектуальных информационных систем и защиты информации	**Знает** принципы построения информационных систем, методов обработки больших данных, особенности построения интеллектуальных информационных систем и защиты информации

3. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина относится к части, формируемой участниками образовательных отношений основной профессиональной образовательной программы специалитета по специальности 27.05.01 «Специальные организационно-технические системы» специализация «Информационно-аналитическая деятельность в специальных организационно-технических системах».

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

4.1 Распределение трудоемкости дисциплины по видам работ по семестрам для очной формы обучения

Вид учебной работы	Трудоемкость		
	з.е.	час.	по семестрам
			А
Общая трудоемкость дисциплины по учебному плану	**3**	**108**	108
Контактная работа		**54**	54
Лекции		**20**	20
Практические занятия		**34**	34
Лабораторные работы			
Консультации перед экзаменом			
Самостоятельная работа		**54**	54
Курсовая работа			
Зачёт			
Зачёт с оценкой		+	+
Экзамен			

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

№ п/п	Наименование разделов и тем	Всего часов	Количество часов по видам занятий, в том числе практическая подготовка			Самостоятельная работа	Контроль
			Лекции	Практические занятия	Лабораторные работы		
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Семестр А							
1.	Тема 1. Понятийный и методологический аппарат, нормативная база и стандарты в области информационной безопасности и защиты информации	14	4	4/4**		6	
2.	Тема 2. Система защиты государственной тайны в РФ	12	2	4		6	
3.	Тема 3. Каналы силового деструктивного воздействия на информацию	8	2			6	
4.	Тема 4. Технические каналы утечки информации	8	2			6	
5.	Тема 5. Нетрадиционные информационные каналы	12	2	4		6	
6.	Тема 6. Криптографическая защита информации	20	2	12		6	

7.	Тема 7. Методы и средства разграничения и контроля доступа к информации	12	2	6		6	
8.	Тема 8. Компьютерная преступность	12	2	4		6	
9.	Тема 9. Ответственность за нарушения и преступления в сфере информационной безопасности	10	2			6	
10.	Зачет с оценкой	+					+
Итого		**108**	**20**	**34/4***		**54**	

**** практическая подготовка при реализации дисциплин организуется путем проведения практических и семинарских занятий, лабораторных работ, предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью***
***** где 2 часа – практическая подготовка***

4.3 Содержание дисциплины для очной формы обучения

Тема 1. Понятийный и методологический аппарат, нормативная база и стандарты в области информационной безопасности и защиты информации»

Лекция. Основные термины и определения в сфере информационной безопасности и защиты информации. «Ландшафт» информационной безопасности: взаимодействие базовых элементов теории. Нормативно-правовая база и стандарты в области информационной безопасности и защиты информации.

Практическая подготовка. Семантический анализ базовых понятий предметной области. Предметный анализ стандартов в области информационной безопасности и защиты информации.

Самостоятельная работа. Абстрактная модель системы защиты информации: основные понятия. Основы формальной теории защиты информации. Модели дискреционного доступа. Модели мандатного доступа. Ролевые модели доступа. Модели безопасности информационных потоков. Акты регуляторов в сфере защиты информации

Рекомендуемая литература

основная: [1,2]

дополнительная: [1-7]

Тема 2. Система защиты государственной тайны в РФ

Лекция. Законодательство Российской Федерации о государственной тайне. Перечень сведений, составляющих государственную тайну. Степени секретности сведений и грифы секретности носителей. Порядок отнесения сведений к государственной тайне. Допуск должностных лиц и граждан к государственной тайне. Структура системы защиты государственной тайны. Ответственность за нарушения законодательства в области защиты государственной тайны.

Практическое занятие. Институт «тайны» в Российском законодательстве.

Самостоятельная работа. Краткая история защиты информации в России.

Рекомендуемая литература

основная: [1,2]

дополнительная: [1-7]

Тема 3. Каналы силового деструктивного воздействия на информацию

Лекция. Канал силового деструктивного воздействия (СДВ) на информацию по сети электропитания. Канал СДВ по проводным линиям. Канал СДВ по «эфиру». Классификация средств СДВ. Рекомендации по защите компьютерных систем от СДВ.

Самостоятельная работа. Электромагнитный спектр как источник воздействия на информацию

Рекомендуемая литература

основная: [1,2]

дополнительная: [1-7]

Тема 4. Технические каналы утечки информации

Лекция. 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 (акустооптическому) каналу.

Самостоятельная работа. Средства обнаружения технических каналов утечки информации. Средства препятствования утечке информации по техническим каналам. 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: [1-7]

Тема 5. Нетрадиционные информационные каналы

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

Практическое занятие. Сокрытие информации в печатном тексте.

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

Рекомендуемая литература

основная: [1,2]

дополнительная: [1-7]

Тема 6. Криптографическая защита информации

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

Практическое занятие. Криптография и криптоанализ шифров перестановки. Криптография и криптоанализ шифров простой замены. Криптоанализ шифра Виженера. Криптоанализ блочного шифра AES. Криптография с открытым ключом: атаки на алгоритм RSA.

Самостоятельная работа. Электронная подпись

Рекомендуемая литература

основная: [1,2]

дополнительная: [1-7]

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

Лекция. Процедура идентификации, аутентификации и авторизации. Система паролирования.

Практическое занятие. Создание защищенных учетных записей. Защита электронных документов.

Самостоятельная работа. Система контроля и управления доступом (СКУД). Система охраны периметра

Рекомендуемая литература

основная: [1,2]

дополнительная: [1-7]

Тема 8. Компьютерная преступность

Лекция. Классификация компьютерных преступлений. Понятие компьютерной преступности. Масштабы и общественная опасность компьютерной преступности. Виды и субъекты компьютерных преступлений.

Практическое занятие. Кодификатор Интерпола.

Самостоятельная работа. Специфика расследования компьютерных преступлений

Рекомендуемая литература

основная: [1,2]

дополнительная: [1-7]

Тема 9. Ответственность за нарушения и преступления в сфере информационной безопасности

Лекция. 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.

Самостоятельная работа. Права регуляторов в части наложения административных взысканий за нарушения в сфере информационной безопасности и защиты информации

Рекомендуемая литература

основная: [1,2]

дополнительная: [1]

5. Методические рекомендации по организации изучения дисциплины

При реализации программы дисциплины «Базы данных» 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:

- систематизированные основы научных знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей области науки и техники;
- концентрировать внимание обучающихся на наиболее сложных и узловых вопросах;
- стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления.

В ходе практического занятия обеспечивается процесс активного взаимодействия обучающихся с преподавателем; приобретаются практические навыки и умения. Цели практического занятия: выработка практических умений и приобретение навыков, закрепление пройденного материала по соответствующей теме дисциплины.

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 опроса / 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

По теме 1:

- дайте определение основным терминам в сфере информационной безопасности и защиты информации (угроза, уязвимость, конфиденциальность, целостность, доступность);
- назовите основные стандарты в области информационной безопасности и защиты информации;
- назовите регуляторов в сфере защиты информации и их основные нормативно-правовые акты;
- перечислите и дайте определение основным моделям доступа.

По теме 2:

- перечислите элементы структуры системы защиты государственной тайны;
- назовите регуляторов в сфере защиты государственной тайны и зоны их ответственности;
- перечислите порядок допуска должностных лиц и граждан к государственной тайне;
- назовите закон, регулирующий отношения в области защиты государственной тайны, и его основные новации.

По теме 3:

- назовите типы каналов силового деструктивного воздействия на информационную систему;
- перечислите пути проникновения всплеска энергии для каждого из типов каналов силового деструктивного воздействия;
- назовите основные рекомендации по защите компьютерных систем от силового деструктивного воздействия.

По теме 4:

- приведите классификацию технических каналов утечки информации;
- дайте определение технических каналов утечки информации (ПЭМИН, радиоканал, электрический, виброакустический, акустоэлектрический; параметрический, акустооптический);

- перечислите организационные меры, препятствующие утечке информации по техническим каналам;
- перечислите технические меры, препятствующие утечке информации по техническим каналам;
- приведите примеры электронных устройств негласного получения информации;
- назовите ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации

По теме 5:

- дайте определение нетрадиционного информационного канала;
- назовите отличие криптографии от стеганографии;
- назовите методы сокрытия информации в файлах (текстовых, звуковых, графических);
- дайте характеристику методов сокрытия информации в файлах (объем, скрытность, сложность).

По теме 6:

- приведите классификацию шифров;
- назовите отличие криптосистем с симметричными и несимметричными ключами;
- приведите примеры криптографических алгоритмов;
- дайте определение электронной подписи;
- назовите основные стандарты шифрования.

По теме 7:

- дайте определение основным терминам системы паролирования (идентификации, аутентификации и авторизации);
- перечислите основные типы атак на систему паролирования;
- назовите признаки «идеального» пароля;
- перечислите структурные элементы системы контроля и управления доступом;
- перечислите структурные элементы системы охраны периметра.

По теме 8:

- приведите классификацию компьютерных преступлений;
- назовите масштабы компьютерной преступности;
- приведите структуру кодификатора Интерпола;
- раскройте специфику расследования компьютерных преступлений.

По теме 9:

- назовите виды ответственности за нарушения в сфере информационной безопасности и защиты информации;
- перечислите статьи Уголовного кодекса РФ в части ответственности за преступления в сфере компьютерной информации;
- назовите статью Уголовного кодекса РФ, регламентирующую ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации.

- приведите права регуляторов в части наложения административных взысканий за нарушения в сфере информационной безопасности и защиты информации

Типовые задания для тестирования

По теме 1:

1) Расположите уровни обеспечения информационной безопасности в РФ от высшего к низшему.

2) Что или кто НЕ является элементом системы обеспечения информационной безопасности РФ?

3) Угроза информационной безопасности - это...

4) Уязвимость - это...

5) Актив - это...

6) Конфиденциальность информации - это...

7) Целостность информации - это...

8) Доступность информации - это...

9) Регуляторами в сфере защиты информации являются...

10) Какая модель доступа предполагает наличие матрицы доступа?

По теме 2: ГТ

1) Какие новации содержит «Закон о государственной тайне»

2) Границы действия «Закона о государственной тайне»

3) Кто наделен полномочиями по отнесению сведений к государственной тайне?

4) Не подлежит засекречиванию информация о...

5) Какой степени секретности НЕ существует?

6) Основанием для отказа должностному лицу или гражданину в допуске к государственной тайне могут являться...

7) К органам защиты государственной тайны относятся...

8) Государственную тайну составляют сведения...

9) Условием прекращения допуска к государственной тайне является...

10) Полномочия Межведомственной комиссии по защите государственной тайны...

11) Полномочия По теме 3:

1) Кейс с электролитическими конденсаторами включили в сетевую розетку офисной ЛВС. Определите канал силового деструктивного воздействия (КСДВ).

2) Кейс с электролитическими конденсаторами включили в офисную розетку сети электропитания. Определите КСДВ.

3) Электрошокер воткнули в сетевой разъем маршрутизатора. Определите КСДВ.

4) Резонирующий емкостной накопитель подключили ко вторичной обмотке трансформаторной подстанции. Определите КСДВ.

5) Мощный разряд молнии в непосредственной близости. Определите КСДВ.

6) Внедрение программной закладки в источник бесперебойного питания. Определите КСДВ.

7) Электромагнитный импульс от генератора СВЧ-излучения, установленного в багажнике легкового автомобиля. Определите КСДВ.

8) Прокладка мощного кабеля электропитания сварочного аппарата в одном коробе с кабелем ЛВС. Определите КСДВ.

9) Сварочные работы вблизи включенного системного блока. Определите КСДВ.

10) Подключение сварочного аппарата в офисную розетку сети электропитания. Определите КСДВ.

По теме 4:

1) Перехват побочных электромагнитных излучений от работы персонального компьютера. Выберите тип технического канала утечки информации (ТКУИ), соответствующий инциденту информационной безопасности.

2) Перехват речевой информации путём ВЧ-облучения пассивного закладного устройства. Выберите тип ТКУИ.

3) Наводки информационных сигналов в посторонних проводниках (фидерах). Выберите тип ТКУИ.

4) Перехват речевых сигналов направленными микрофонами. Выберите тип ТКУИ.

5) Приём информации, передаваемой закладными устройствами по электросети 220 В. Выберите тип ТКУИ.

6) Беспроводной прием информации, передаваемой закладными устройствами. Выберите тип ТКУИ.

7) Перехват речевых сигналов контактными микрофонами (стетоскопами). Выберите тип ТКУИ.

8) Приём отражённого от оконного стекла лазерного излучения, модулированного речевым сигналом. Выберите тип ТКУИ.

9) Перехват речевых сигналов через вспомогательные технические средства и иные устройства, обладающие «микрофонным эффектом». Выберите тип ТКУИ.

10) «Просачивание» информативных сигналов в линии электропитания технических средств обработки информации. Выберите тип ТКУИ.

По теме 5: Стего

1) Сколько страниц текстовой информации (2000 символов/страница) может быть сокрыто методами стеганографии в мегапиксельной фотографии формата bmp?

2) Сколько страниц текстовой информации может быть сокрыто методами стеганографии в 30 секундах монозвучания файла формата wav?

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

4) Сколько страниц текстовой информации может быть сокрыто методами стеганографии в 1 странице текстового файла?

5) В текстовом файле на каком языке – на русском или на английском – можно сокрыть больше цифровой информации, используя символы-«оборотни»?

6) Сколько страниц текстовой информации (2000 символов/страница) может быть сокрыто методами стеганографии в электронном 300-страничном томике У. Шекспира на языке оригинала?

7) Сколько страниц текстовой информации (2000 символов/страница) может быть сокрыто методами стеганографии в в электронном 300-страничном томике А.С. Пушкина?

8) Расположите следующие файлы по объему скрываемой цифровой информации (от большего к меньшему): электронная библиотека (100 томов), музыкальный альбом (100 песен), свадебный фотоальбом (100 фото), видеофильм (100 минут). Выберите вариант.

9) Несовершенство чего в организме пользователя эксплуатируется злоумышленниками при сокрытии цифровой информации в файлах?

10) Нетрадиционный информационный канал – это...

По теме 6: Крипто

1) Криптография – это...
2) Криптоанализ – это...
3) Криптология – это...
4) При криптографии изменяется...
5) Шифр «Цезаря» заключается в замене символов исходного сообщения символами того же алфавита, но смещенными на определенное количество позиций по алфавиту вправо. Какое слово было зашифровано, если получилось «ДГОДЗФ»?
6) Как размер криптограммы влияет на успешность и время дешифровки?
7) Сообщение какого объема можно зашифровать, используя «Решетку Кардано» с 15 прорезями для букв?
8) Сообщение какого максимального объема можно зашифровать, используя «Решетку Кардано» 10х10?
9) Определите размер хэша 1 мегабайта текста для алгоритма MD-5
10) Какой шифр является блочным: RSA или AES?

По теме 7: Пароли

1) Для чего служат пароли (в компьютерной системе)?
2) Идентификация (в компьютерной системе) - это...
3) Аутентификация (в компьютерной системе) - это...
4) Авторизация (в компьютерной системе) - это...
5) В каком виде пароли хранятся в современной компьютерной системе?
6) Мониторинг трафика Интернет-банкинга». Укажите тип атаки на парольную систему.
7) «Телефонный звонок от имени системного администратора». Укажите тип атаки на парольную систему.

8) «Сбор персональных данных пользователя». Укажите тип атаки на парольную систему.

9) «Переадресация на подставной сайт банка». Укажите тип атаки на парольную систему.

10) Использование каких приемов усиливает стойкость парольной систем от взлома?

По темам 8-9:

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

2) 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...

3) 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...

4) Выбрав определенную компанию, хакеры рассылали ее сотрудникам электронные письма с программой Poison Ivy, которая при открытии вложения инсталлировалась в систему и отсылала по зашифрованному каналу информацию о внутренней сети предприятия. Укажите класс вредоносной программы.

5) Отказ в доступе к среде передачи, в установлении соединения, в предоставлении сервиса. Укажите возможную причину (класс сетевой атаки).

6) «По мнению обвинения 4 гражданам России грозит 5 лет лишения свободы и штраф в $250 000 за угадывание с помощью смартфонов алгоритма действий игрового автомата Aristocrat Mark VI более чем в 10 казино в США». Присвойте этому компьютерному преступлению код Интерпола.

7) Незаконный оборот специальных технических средств, предназначенных для негласного получения информации, наказывается...

8) За неправомерный доступ к компьютерной информации предусматривается...

9) Максимальный срок лишения свободы за создание «троянской программы»…

10) Максимальный срок лишения свободы за мошенничество в сфере компьютерной информации, совершенное организованной группой либо в особо крупном размере ...

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 раскры-	отлично

		ты основные положения вопросов; могут быть допущены недочеты, исправленные самостоятельно в процессе ответа.	
		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 нарушения; в ответе отсутствуют выводы.	удовлетворительно
		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

7.1 Лицензионное и свободно распространяемое программное обеспечение

Перечень лицензионного и свободно распространяемого программного обеспечения:

- Astra Linux Common Edition, Операционная система общего назначения, номер в Едином реестре российских программ для электронных вычислительных машин и баз данных – 4433, лицензия на право пользования № 217800111-ore-2.12-client-6196.

- Яндекс Браузер для организаций (бесплатный функционал) [ПО-С52 373]. Браузер позволяет общаться с Голосовым помощником Алисой, фильтрует рекламу, защищает личные данные. Номер в Едином реестре российских программ для электронных вычислительных машин и баз данных – 3722, свободный доступ.

- Мой Офис Образование [ПО-41В-124]. Полный комплект редакторов текстовых документов и электронных таблиц, а также инструментарий для работы с графическими презентациями. Номер в Едином реестре российских программ для электронных вычислительных машин и баз данных – 4557, свободный доступ.

7.2. Профессиональные базы данных и информационные справочные системы

1. Сервер органов государственной власти Российской Федерации http://россия.рф/ (свободный доступ);
2. Портал открытых данных Российской Федерации https://data.gov.ru/ (свободный доступ);
3. Федеральный портал «Российское образование» http://www.edu.ru (свободный доступ);
4. Система официального опубликования правовых актов в электронном виде http://publication.pravo.gov.ru (свободный доступ);
5. Федеральный портал «Совершенствование государственного управления» https://ar.gov.ru (свободный доступ);
6. Электронная библиотека университета http://elib.igps.ru (авторизованный доступ);
7. Электронно-библиотечная система «ЭБС IPR BOOKS» http://www.iprbookshop.ru (авторизованный доступ).
8. Электроно-библиотечная система "Лань" https://e.lanbook.com (авторизованный доступ).

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. Крылов, Г. О. Понятийный аппарат информационной безопасности : словарь / Г. О. Крылов, С. Л. Ларионова, В. Л. Никитина. – Москва, Саратов : Всероссийский государственный университет юстиции (РПА Минюста России), Ай Пи Эр Медиа, 2016. – 343 с. – ISBN 978-5-00094-308-3. – Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. – URL:

https://www.iprbookshop.ru/64306.html. – Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/64306

2. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2024. — 266 с. — ISBN 978-5-4497-3316-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/142285.html . — Режим доступа: для авторизир. пользователей

3. Литвиненко, О. В. Правовые аспекты информационной безопасности : учебное пособие / О. В. Литвиненко. – Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2021. – 63 с. – Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprbookshop.ru/125273.html . – Режим доступа: для авторизир. пользователей

4. Дронов, В. Ю. Международные и отечественные стандарты по информационной безопасности : учебно-методическое пособие / В.Ю. Дронов. – Новосибирск : Новосибирский государственный технический университет, 2016. – 34 с. – ISBN 978-5-7782-3112-2. – Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprbookshop.ru/91395.html . – Режим доступа: для авторизир. пользователей

5. Овчинникова, Е. А. Организационно-правовые основы информационной безопасности. Ч.1 : учебное пособие / Е. А. Овчинникова, Г. В. Попков ; под редакцией С. Н. Новикова. – Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2022. – 193 с. – Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprbookshop.ru/138773.html . – Режим доступа: для авторизир. пользователей

6. Овчинникова, Е. А. Организационно-правовые основы информационной безопасности. Ч.2 : учебное пособие / Е. А. Овчинникова, Г. В. Попков ; под редакцией С. Н. Новикова. – Новосибирск : Сибирский государственный университет телекоммуникаций и информатики, 2022. – 168 с. – Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. – URL: https://www.iprbookshop.ru/138774.html . – Режим доступа: для авторизир. Пользователей

7. Введение в информационную безопасность и защиту информации : учебное пособие / В. А. Трушин, Ю. А. Котов, Л. С. Левин, К. А. Донской. — Новосибирск : Новосибирский государственный технический университет, 2017. — 132 с. — ISBN 978-5-7782-3233-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/91329.html . — Режим доступа: для авторизир. пользователей

7.4. Материально-техническое обеспечение

Занятия по дисциплине проводятся в специальных помещениях представляющие собой учебные аудитории для проведения занятий лекционного

типа, занятий семинарского типа, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.

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

На ряде практических занятий используется компьютерный класс, оборудованный ПК, объединенными в локальную вычислительную сеть и имеющими доступ к сети Интернет.

Авторы: д.т.н., профессор Буйневич М.В., к.т.н., доцент Максимов А.В.