ФГБОУ ВО «Санкт-Петербургский университет ГПС МЧС России»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ И ЗАЩИТА ИНФОРМАЦИИ

Бакалавриат по направлению подготовки
27.03.03 Системный анализ и управление
направленность (профиль) «Системный анализ и управление в организационно-технических системах»

Санкт-Петербург

1. Цель и задачи дисциплины «Безопасность информационных систем и защита информации»

Цели освоения дисциплины «Безопасность информационных систем и защита информации»:

- 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-2	способность эксплуатировать системы управления, применять современные инструментальные средства и технологии программирования на основе профессиональной подготовки, обеспечивающие решение задач системного анализа и управления

Задачи дисциплины «Безопасность информационных систем и защита информации»:

- 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 «Безопасность информационных систем и защита информации», соотнесенных с планируемыми результатами освоения образовательной программы

Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
Категория (группа) общепрофессиональных компетенций: эксплуатация системно-аналитических комплексов и их компонент	
Владеет навыками сбора, обобщения и анализа больших данных, защиты информации, используя современные инструментальные средства ПК-2.3	Знает
	структуры и основных положений системы защиты государственной тайны, основных каналов реализации угроз безопасности информации, базовые методы и средства защиты информации от несанкционированного доступа, современного состояния компьютерной преступности и ответственности за нарушения и преступления в сфере информационной безопасности ПК-2.3
	Умеет
	идентифицировать основные угрозы безопасности современных информационных систем, создавать защищенные учетные записи и защищать электронные документы, классифицировать компьютерные преступления ПК-2.3

3. Место дисциплины «Безопасность информационных систем и защита информации» в структуре ОПОП

Дисциплина относится к части, формируемой участниками образовательных отношений основной профессиональной образовательной программы бакалавриата по направлению подготовки 27.03.03 -Системный анализ и управление направленность (профиль) «Системный анализ и управление в организационно-технических системах».

4. Структура и содержание дисциплины «Безопасность информационных систем и защита информации»

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

4.1 Распределение трудоемкости учебной дисциплины «Безопасность информационных систем и защита информации» по очной форме обучения и видам работ

Вид учебной работы	Трудоемкость		
	з.е.	час.	семестр
			7
Общая трудоемкость дисциплины по учебному плану	**3**	**108**	**108**
Контактная работа, в том числе:		**54**	**54**
Аудиторные занятия		**54**	**54**
Лекции (Л)		20	20
Практические занятия (ПЗ)		34	34
Самостоятельная работа (СРС)		**54**	**54**
Зачет с оценкой		+	+

4.2 Разделы и темы дисциплины «Безопасность информационных систем и защита информации» и виды занятий

№ 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**
Раздел 1. Понятийный и методологический аппарат, нормативная база и стандарты в области информационной безопасности и защиты информации							
1.	Тема 1. Понятийный и методологический аппарат, нормативная база и стандарты в области информационной безопасности и защиты информации	14	4	4		6	
2.	Тема 2. Система защиты государственной тайны в РФ	12	2	4		6	
Раздел 2. Каналы реализации угроз безопасности информации							
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	
Раздел 3. Методы и средства защиты информации от несанкционированного доступа							
6.	Тема 6. Криптографическая защита информации	18	2	10		6	
7.	Тема 7. Методы и средства разграничения и контроля доступа к информации	12	2	4		6	
Раздел 4. Компьютерная преступность, ответственность за нарушения и преступления в сфере							

информационной безопасности							
8.	Тема 8. Компьютерная преступность	12	2	4		6	
9.	Тема 9. Ответственность за нарушения и преступления в сфере информационной безопасности	12	2	4		6	
10.	Зачет с оценкой	+					+
Итого		**108**	**20**	**34**		**54**	

4.3 Тематический план для обучающихся

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

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]

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]

РАЗДЕЛ 2. КАНАЛЫ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

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]

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]

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: [1,3,4]

РАЗДЕЛ 3. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

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: [1,2]

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]

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

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]

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 «Безопасность информационных систем и защита информации»

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 «Безопасность информационных систем и защита информации»

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

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

1) морально-этический, организационно-технический, программно-аппаратный, духовно-нравственный, нормативно-правовой
2) духовно-нравственный, морально-этический, нормативно-правовой, организационно-технический, программно-аппаратный
3) нормативно-правовой, организационно-технический, морально-этический, программно-аппаратный, духовно-нравственный
4) духовно-нравственный, морально-этический, организационно-технический, программно-аппаратный, нормативно-правовой

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

1) Федеральное Собрание
2) Президент
3) органы местного самоуправления
4) Общественная палата
5) органы исполнительной власти
6) Совет безопасности

Кто наделен полномочиями по отнесению сведений к государственной тайне?

1) министр сельского хозяйства
2) руководитель Федеральной таможенной службы
3) руководитель Росгидромета
4) председатель Банка РФ

Не подлежит засекречиванию информация о

1) состоянии окружающей среды
2) состоянии здоровья премьер-министра
3) размерах золотовалютного резерва
4) состоянии борьбы с преступностью
5) привилегиях

Какой степени секретности не существует?

1) государственной важности
2) совершенно секретно
3) особой важности
4) секретно
5) конфиденциально
6) для служебного пользования

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

1) признание его рецидивистом
2) постоянное проживание близких родственников за границей
3) сообщение заведомо ложных анкетных данных
4) наличие медицинских противопоказаний
5) наличие загранпаспорта

К органам защиты государственной тайны относятся...
Федеральная служба безопасности

1) Служба внешней разведки
2) Министерство внутренних дел
3) Федеральная служба по техническому и экспортному контролю
4) Министерство обороны
5) Федеральная служба охраны

Закон «О государственной тайне» действует на территории:

1) только Российской Федерации
2) только Российской Федерации и стран СНГ
3) только Российской Федерации и стран ОДКБ
4) Российской Федерации и за ее пределами

Принципом отнесения сведений к государственной тайне и засекречивания этих сведений НЕ является:

1) обоснованность
2) своевременность
3) добровольность

Обладатель обязан принимать защитные меры по обеспечению конфиденциальности …

1) только информации ограниченного доступа
2) только общедоступной информации
3) информации ограниченного доступа и общедоступной информации

Обладатель обязан принимать защитные меры по обеспечению целостности …

1) только информации ограниченного доступа
2) только общедоступной информации
3) информации ограниченного доступа и общедоступной информации

Носителем сведений, составляющих государственную тайну, могут являться:

1) письменные документы
2) магнитные носители
3) микрочипы
4) граждане РФ
5) граждане иных государств
6) лица без гражданства

Допуск к государственной тайне - это ...

1) процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну
2) процедура оформления права предприятий, учреждений и организаций на проведение работ с использованием сведений, составляющих государственную тайну

3) санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну

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 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 «Безопасность информационных систем и защита информации»

7.1. Лицензионное и свободно распространяемое программное обеспечение отечественного производства

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

- Astra Linux Common Edition релиз Орел [ПО-25В-603] - Операционная система общего назначения "Astra Linux Common Edition" [Коммерческая

(Full Package Product). Номер в Едином реестре российских программ для электронных вычислительных машин и баз данных - 4433]

7.2. Профессиональные базы данных и информационные справочные системы

1. Информационная система «Единое окно доступа к образовательным ресурсам» [Электронный ресурс]. – Режим доступа: http://window.edu.ru/, доступ только после самостоятельной регистрации
2. Научная электронная библиотека «eLIBRARY.RU» [Электронный ресурс]. – Режим доступа: https://www.elibrary.ru/, доступ только после самостоятельной регистрации
3. Электронная библиотека Санкт-Петербургского университета ГПС МЧС России: http://elib.igps.ru
4. Электронно-библиотечная система IPRBOOK: http://www.iprbookshop.ru/
5. Электронно-библиотечная система ЛАНЬ: 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 «Безопасность информационных систем и защита информации»

Для проведения и обеспечения занятий используются помещения, которые представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой бакалавриата, 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.