ФГБОУ ВО «Санкт-Петербургский университет ГПС МЧС России»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специалитет по специальности
10.05.03 – Информационная безопасность автоматизированных систем

Специализация «Анализ безопасности информационных систем»

Санкт-Петербург

1. Цели и задачи дисциплины

Цель освоения дисциплины: получение обучающимися необходимых знаний и навыков в области теории обеспечения информационной безопасности, правового и организационного обеспечения информационной безопасности, законодательства в области интеллектуальной собственности, персональных данных, коммерческой и государственной тайны, электронной цифровой подписи.

Перечень компетенций, формируемых в процессе изучения дисциплины

Компетенции	Содержание
ОПК - 5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации;
ОПК - 6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;
ОПК – 7.2	Способен разрабатывать методики и тесты для анализа степени защищенности информационной системы и ее соответствия нормативным требованиям по защите информации;

Задачи дисциплины:

- изложить основы информационного законодательства Российской Федерации;
- представить знания о компьютерных преступлениях;
- раскрыть основы организационного обеспечения безопасности информации.

2. Перечень планируемых результатов обучения дисциплины, соотнесенных с индикаторами достижения компетенций

Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-5.1. Использует основные нормативные правовые акты, стандарты и методические документы в области защиты информации и информационной безопасности	**Знает** основные нормативные правовые акты в области информационной безопасности и защиты информации **Умеет** применять нормативные правовые акты и нормативные методические документы в области защиты информации
ОПК-5.2. Применяет нормативные акты при проектировании и разработке систем безопасности автоматизированных информационных систем и их компонентов	**Знает** нормативные методические документы, регламентирующие порядок выполнения мероприятий по защите информации в автоматизированной информационной системе
ОПК-6.3. Применяет действующую нормативную базу, нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю для организации защиты информации ограниченного доступа в автоматизированных системах	**Знает** нормативные документы в области обеспечения защиты информации ограниченного доступа
ОПК-7.2.1. Использует знания источников и классификации угроз информационной безопасности; нормативные документы, стандарты, содержащие рекомендации и требования по использованию методов и средств защиты информации; методы и средства анализа программного обеспечения информационных систем	**Умеет** предлагать обоснованные варианты организационного обеспечения безопасн6ости информации на конкретных объектах информационной защиты**;** разрабатывать предложения по совершенствованию системы управления информационной безопасностью
ОПК-7.2.2. Демонстрирует способности применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности для анализа степени защищенности информационной системы; проводить мониторинг угроз безопасности компьютерных сетей и систем	**Умеет** проводить анализ степени защищенности информационной системы; использовать существующие нормативно-правовые акты и нормативные методические документы для решения практических задач в том числе при мониторинге угроз информационной безопасности

3. Место дисциплины в структуре ОПОП

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к обязательной части, образовательной программы специалитета по специальности **10.05.03** –

Информационная безопасность автоматизированных систем, специализация **Анализ безопасности информационных систем.**

4. Структура и содержание

Дисциплина «Организационное и правовое обеспечение информационной безопасности» реализуется:

Для очной формы обучения в рамках обязательной части образовательной программы в объеме 180 академических часов (5 зачетных единиц).

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

Вид учебной работы	Трудоемкость			
	з.е.	час.	по семестрам	
			7	8
Общая трудоемкость дисциплины по учебному плану	**5**	**180**	**72**	**108**
Контактная работа, в том числе:		**74**	**36**	**38**
Аудиторные занятия		**72**	**36**	**36**
Лекции (Л)		32	16	16
Практические занятия (ПЗ)		40	20	20
Консультация		**2**		**2**
Самостоятельная работа (СРС)		**70**	**36**	**34**
Зачет с оценкой			+	
Экзамен		**36**		**36**

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

Наименование разделов и тем	**Всего часов**	**Количество часов по видам занятий**					**Самостоятельная работа**
		Лекции	**Практические занятия**	**Практическая подготовка**	**Консультации**	**Контроль**	
7 семестр							
Основы теории обеспечения информационной безопасности	36	8	10				18
Правовое обеспечение информационной безопасности	36	8	4	6			18

Зачет с оценкой						+	
Итого за 7 семестр	**72**	**16**	**14**	**6**			**36**
8 семестр							
Организационное обеспечение информационной безопасности	24	16	20				34
Консультации	2				2		
Экзамен	36					36	
Итого за 8 семестр	**108**	**16**	**20**		**2**	**36**	**34**
Всего за 7,8 семестр	**180**	**34**	**34**	**6**	**2**	**36**	**70**

4.3 Содержание дисциплины для очной формы обучения

Раздел 1. Основы теории обеспечения информационной безопасности

Лекции. Информационное общество и его безопасность. Информация – фактор существования и развития общества. Обеспечение информационной безопасности: содержание и структура понятия. Система обеспечения информационной безопасности.

Практические занятия. Задачи и методы обеспечения информационной безопасности.

Самостоятельная подготовка. Актуальные проблемы создания и совершенствования системы защиты информации. Понятия доступности, целостности и конфиденциальности, их смысл в контексте проблемы информационной безопасности.

Рекомендуемая литература:

основная [1, 2];

дополнительная [1,2,3]

Раздел 2. Правовое обеспечение информационной безопасности

Лекции. Информационная безопасность государства. Нормативные правовые акты Российской Федерации в области информации, информационных технологий и защиты информации. Конституционные права граждан на информацию и возможности их ограничения.

Практические занятия. Защита информации, содержащейся в информационных системах общего пользования.

Практическая подготовка. Работа с нормативными документами в области защиты информации. Разработка базового блока документов для обеспечения информационной безопасности. Технология цифровой электронной подписи.

Самостоятельная подготовка. Государственная тайна как особый вид защищаемой информации. Законодательство Российской Федерации в области защиты государственной тайны.

Рекомендуемая литература:

основная: [1,2];
дополнительная: [1,2,3]

Раздел 3. Организационное обеспечение информационной безопасности

Лекции. Цели, задачи и субъекты информационной безопасности. Организационная структура системы обеспечения информационной безопасности. Основные мероприятия по созданию и обеспечению функционирования комплексной системы защиты информации.

Практические занятия. Защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем. Имитационное моделирование. Компоненты модели информационной безопасности на 1 уровне.

Самостоятельная подготовка. Организационно-распорядительные документы по обеспечению информационной безопасности. Концепция и политики информационной безопасности на предприятии (в организации).

Рекомендуемая литература:
основная [1, 2,];
дополнительная [1, 2, 3]

5. Методические рекомендации по организации изучения дисциплины «Организационное и правовое обеспечение информационной безопасности»

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:

– 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 «Организационное и правовое обеспечение информационной безопасности»

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

Промежуточная аттестация обеспечивает оценивание промежуточных и окончательных результатов обучения по дисциплине, проводится в форме зачета с оценкой в 7 семестре и экзамена в 8 семестре.

6.1. Примерные оценочные материалы:

6.1.1. Текущего контроля

Типовые вопросы для опроса:

– 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;

– 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.

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.

Примерный перечень вопросов, выносимых на экзамен:

1. Информационное общество и его безопасность.
2. Информация – фактор существования и развития общества.
3. Обеспечение информационной безопасности: содержание и структура понятия.
4. Законодательство о персональных данных.
5. Законодательство в области интеллектуальной собственности
6. Законодательство о коммерческой тайне.
7. Законодательство о государственной тайне.
8. Законодательство об электронной цифровой подписи.
9. Законодательство о техническом регулировании
10. Система обеспечения информационной безопасности
11. Элементы теории права.
12. Основы теории правового обеспечения информационной безопасности
13. Юридическая ответственность.
14. Защита прав и законных интересов субъектов информационной сферы

15. Законодательство об информации, информационных технологиях и о защите информации.

16. Организационные системы обеспечения безопасности информации.

17. Корпоративное нормативное регулирование.

18. Организация объектовых режимов безопасности.

19. Управление персоналом на предприятиях и в организациях.

6.2. Шкала оценивания результатов промежуточной аттестации и критерии выставления оценок

Форма контроля	Показатели оценивания	Критерии выставления оценок	Шкала оценивания
Экзамен, 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 «Организационное и правовое обеспечение информационной безопасности»

7.1. Лицензионное и свободно распространяемое программное обеспечение

Перечень лицензионного и свободно распространяемого программного обеспечения:

- 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. Справочная правовая система «КонсультантПлюс: Студент» [Электронный ресурс]. – Режим доступа: http://student.consultant.ru/, свободный доступ
4. Информационно-правовой портал «Гарант» [Электронный ресурс]. – Режим доступа: http://www.garant.ru/, свободный 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. 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

7.4. Материально-техническое обеспечение

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

Авторы: к.ю.н. Метельков А.Н.