ФГБОУ ВО «Санкт-Петербургский университет ГПС МЧС России»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ

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:

– дисциплина имеет своей целью: обеспечить выполнение требований, изложенных в федеральном государственном образовательном стандарте высшего профессионального образования по специальности подготовки 10.05.03 «Информационная безопасность автоматизированных систем» и познакомить с видами информационной защиты, включая защиту человека от неинформированности и опасной информации. Изучение дисциплины направлено на формирование перечисленных ниже элементов профессиональных компетенций.

Перечень компетенций, формируемых в процессе изучения дисциплины

Компетенции	Содержание
ОПК - 1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства

Задачи дисциплины:

- раскрытие сущности и значения информационной безопасности и защиты информации;
- проанализировать свойства защищаемой информации на различных уровнях ее представления;
- раскрыть общее представление об информационных угрозах;
- изложить содержание различных направлений информационной защиты.

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

Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-1.2. Определяет значение информационных технологий и информационной безопасности для целей государства и общества	**Знает** актуальные проблемы защиты информации, в том числе основные понятия и угрозы **Умеет** на основе полученных знаний самостоятельно разобраться в особенностях построения и функционирования систем защиты информации

3. Место дисциплины в структуре ОПОП

Дисциплина «Введение в специальность» 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 «Введение в специальность» реализуется:

Для очной формы обучения в рамках обязательной части образовательной программы в объеме 72 академических часов (2 зачетных единицы).

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

Вид учебной работы	Трудоемкость		
	з.е.	час.	по семестрам
			1
Общая трудоемкость дисциплины по учебному плану	**2**	**72**	**72**
Контактная работа, в том числе:		**36**	**36**
Аудиторные занятия		**36**	**36**
Лекции (Л)		20	20
Практические занятия (ПЗ)		16	16
Самостоятельная работа (СРС)		**36**	**36**
Зачет			+

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	Консультации	Контроль	
1 семестр						
Организация высшего образования в области информационной безопасности. Информация и информационные ресурсы	36	10	8			18
Основы обеспечения безопасности информации	36	10	8			18
Зачет					+	
Всего за 1 семестр	**72**	**20**	**16**			**36**

4.3 Содержание дисциплины для очной формы обучения
очной формы обучения в 1 семестре:

Тема Организация высшего образования в области информационной безопасности. Информация и информационные ресурсы

Лекции. Правовые основы высшего образования: Конституция РФ об образовании, Законы РФ «Об образовании». Организация высшего образования в РФ. Основные функции Минобразования РФ. Лицензирование, аккредитация и аттестация ВУЗов. Федеральные государственные образовательные стандарты. Ступени образования. Направления подготовки и специальности. Содержание федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 Информационная безопасность автоматизированных систем и 10.05.01 Компьютерная безопасность.

Практические занятия. Понятие информации. Информационные процессы и системы. Информационные ресурсы и технологии. Структура информатики. Меры информации. Качество информации. Виды и формы представления информации в информационных системах.

Самостоятельная работа. Актуальность проблемы обеспечения безопасности автоматизированных систем. Обострение проблемы обеспечения безопасности автоматизированных систем на современном этапе.

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

Тема Основы обеспечения безопасности информации

Лекции. Определение информационной безопасности автоматизированных систем. Субъекты информационных отношений, их безопасность.

Цель защиты автоматизированной системы и циркулирующей в ней информации.

Практические занятия. Лицензирование. Сертификация средств защиты информации и аттестация объектов информатизации.

Самостоятельная работа. Специальные требования и рекомендации по технической защите конфиденциальной информации.

Ответственность за нарушения в сфере защиты информации.

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

5. Методические рекомендации по организации изучения дисциплины «Введение в специальность»

При реализации программы учебной дисциплины используется традиционная образовательная технология, основой которой является системный принцип построения разделов и тем, используются лекционные, практические занятия и лабораторная работа.

На всех лекционных занятиях, целью которых является приобретение знаний, используется мультимедийный проектор с комплектом презентаций.

Общими дидактическими целями практического занятия являются:

- обобщение, систематизация, углубление, закрепление теоретических знаний по конкретным темам учебной дисциплины;
- формирование умений применять полученные знания на практике, реализацию единства интеллектуальной и практической деятельности;
- выработка при решении поставленных задач профессионально значимых качеств: самостоятельность, ответственность, точность, творческая инициатива.

Активно используется самостоятельное выполнение каждым обучающимся учебной группы в течение 2 часов (после изучения теоретического материала каждой темы учебной дисциплины и проведения по ней ряда аудиторных практических занятий) индивидуальных практических заданий по изученной теме. Занятия проводятся в процессе активного взаимодействия с преподавателями.

Цель решения индивидуальных практических заданий - проверка уровня индивидуальной готовности обучающегося к решению практических задач по должностному предназначению на основе материала изученной темы.

Образовательными задачами индивидуальных заданий являются:

- глубокое изучение лекционного материала, изучение методов работы с учебной литературой, получение персональных консультаций у преподавателя;
- решение спектра практических задач, в том числе профессиональных (анализ производственных ситуаций, решение ситуационных задач, и т.п.);
- выполнение вычислений, расчетов;
- работа с нормативными документами, инструктивными материалами, справочниками.

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 «Введение в специальность»

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

Промежуточная аттестация обеспечивает оценивание промежуточных и окончательных результатов освоения дисциплины, проводится в форме зачета.

6.1. Примерные оценочные материалы:

6.1.1. Текущего контроля

Тесты по теме – Введение в специальность с ответами (Правильный вариант ответа отмечен знаком +)

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий

+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

- Хищение жестких дисков, подключение к сети, инсайдерство

+ Перехват данных, хищение данных, изменение архитектуры системы

- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

+ Персональная, корпоративная, государственная

- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности

– своевременное обнаружение, предупреждение:

+ несанкционированного доступа, воздействия в сети

- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

+ Компьютерные сети, базы данных

- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети

+ Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

+ Экономической эффективности системы безопасности

- Многоплатформенной реализации системы

- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

- руководители, менеджеры, администраторы компаний

+ органы права, государства, бизнеса

- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:

+ Установление регламента, аудит системы, выявление рисков

- Установка новых офисных приложений, смена хостинг-компании

- Внедрение аутентификации, проверки контактных данных пользователей

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

Форма контроля	Показатели оценивания	Критерии выставления оценок	Шкала оценивания
зачёт	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.	Зачтено
		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.	Зачтено
		дан недостаточно правильный и полный ответ; логика и последовательность изложения имеют нарушения; в ответе отсутствуют выводы.	Зачтено
		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.	Незачтено

7. Ресурсное обеспечение дисциплины «Введение в специальность»

7.1. Лицензионное и свободно распространяемое программное обеспечение

Перечень лицензионного и свободно распространяемого программного обеспечения:

- Статистическая диалоговая система STADIA [ПО-6FF-561] - Статистическая диалоговая система [Лицензионное. Номер в Едином реестре российских программ для электронных вычислительных машин и баз данных - 9064]

- SMath Studio [ПО-A68-516] - Программное обеспечение для вычисления математических выражений и построения графиков функций [Свободно распространяемое. Номер в Едином реестре российских программ для электронных вычислительных машин и баз данных - 12849]

- МойОфис Образование [ПО-41B-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-25B-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. 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

2. 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

3. 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

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.