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:

- формирование у обучающихся целостного представления об информационной безопасности и защите информации как сфере образовательной и профессиональной деятельности;
- формирование у обучающихся понятийного аппарата информационной безопасности и защите информации как фундаментальной базы освоения специальности;

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:

- изучение нормативных правовых и руководящих документах в области информационной безопасности и защиты информации, необходимых для текущей образовательной и дальнейшей профессиональной деятельности;
- изучение обучающимися ответственности за нарушения и преступления в сфере информационной безопасности и защиты информации как частью информационной культуры высокообразованной личности;
- изучение мотивации профессионального развития.

2. Перечень планируемых результатов дисциплины, 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:** – сферу приложения знаний и содержание обучения специалистов по информационной безопасности и защите информации; – основные правила компьютерной «гигиены»; – меру ответственности за нарушения и преступления в сфере информационной безопасности и защиты информации **Умеет** ориентироваться в нормативно-правовой базе в области информационной безопасности и защиты информации **Владеет** понятийным аппаратом информационной безопасности и защиты информации

3. Место дисциплины в структуре основной профессиональной образовательной программы

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 дисциплины

Общая трудоемкость дисциплины составляет 2 зачётные единицы, 72 часа.

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		**36**	**36**
Лекции		20	20
Практические занятия		16	16
Самостоятельная работа		**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						
Тема 1. Понятийный аппарат и нормативно-правовое обеспечение информационной безопасности и защиты информации	24	8	4			12
Тема 2. Компьютерная преступность, ответственность за нарушения и преступления в сфере информационной безопасности и защиты информации	22	6	4			12
Тема 3. Профессиональная и образовательная деятельность в сфере информационной безопасности и защиты информации	26	6	8			12
Зачет					+	
Итого	**72**	**20**	**16**			**36**

4.3 Содержание дисциплины для очной формы обучения

Тема 1. Понятийный аппарат и нормативно-правовое обеспечение информационной безопасности и защиты информации

Лекции. Основные понятия и сущности информационной безопасности и защиты информации; онтологическая модель предметной области. Классификация угроз безопасности информации. Иерархическая система нормативных правовых актов Российской Федерации в сфере информационной безопасности и защиты информации. Система стандартов по информационной безопасности и защите информации.

Практические занятия. Предметный анализ и сущностная разметка руководящих и нормативных документов в области обеспечения информационной безопасности и защиты информации. Табличный анализ результатов.

Самостоятельная работа. Акты Регуляторов в сфере информационной безопасности и защиты информации. История защиты информации. Институт «тайны» в Российском законодательстве.

Рекомендуемая литература:

Основная литература: [1, 2];

Дополнительная литература: [1–4]

Тема 2. Компьютерная преступность, ответственность за нарушения и преступления в сфере информационной безопасности и защиты информации

Лекции. Компьютерная преступность: понятие, статистика, масштабы и общественная опасность; виды и субъекты компьютерных преступлений. Дисциплинарная ответственность за разглашение охраняемой законом тайны. Административная ответственность за нарушения в сфере информационной безопасности и защиты информации. Уголовная ответственность за преступления в сфере компьютерной информации.

Практические занятия. Классификация компьютерных преступлений. Кодификатор Интерпола.

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

Рекомендуемая литература:

Оосновная литература: [1, 2];

Дополнительная литература: [5, 6]

Тема 3. Профессиональная и образовательная деятельность в сфере информационной безопасности и защиты информации

Лекции. Сфера приложения знаний специалистов по информационной безопасности и защите информации. Профессиональные стандарты в области информационной безопасности и защиты информации. Структура образования и образовательные стандарты по направлению информационная безопасность и защита информации. Содержание обучения по специальности «Информационная безопасность автоматизированных систем», специализация – «Анализ безопасности информационных систем». Основные правила компьютерной «гигиены», парольная политика.

Практические занятия. Построение семантической сети знаний в области информационной безопасности и защиты информации.

Самостоятельная работа. Система подготовки специалистов по информационной и кибербезопасности в зарубежных государствах.

Рекомендуемая литература:

Оосновная литература: [1, 2];

Дополнительная литература: [7]

5. Методические рекомендации по организации изучения дисциплины

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

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.);
- 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

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) Выберите правильный порядок уровней обеспечения информационной безопасности в РФ от высшего к низшему

– морально-этический, организационно-технический, программно-аппаратный, духовно-нравственный, нормативно-правовой

+ духовно-нравственный, морально-этический, нормативно-правовой, организационно-технический, программно-аппаратный

– нормативно-правовой, организационно-технический, морально-этический, программно-аппаратный, духовно-нравственный;

– духовно-нравственный, морально-этический, организационно-технический, программно-аппаратный, нормативно-правовой

2) Основными Регуляторами в сфере информационной безопасности и защиты информации в России являются

+ ФСТЭК

– МВД

+ ФСБ

– Совет безопасности

+ Роскомнадзор

3) Как называется процесс проверки подлинности пользователя информационной системы?

– идентификация

+ аутентификация

– авторизация

4) Какой тайны не существует?

+ военной

– коммерческой

– банковской

– нотариальной

– следствия

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

– Федеральное Собрание

– Президент

– органы местного самоуправления

+ Общественная палата

– органы исполнительной власти

– Совет безопасности

6) Основными рисками информационной безопасности является ущерб какому свойству информации?

+ конфиденциальности

– полноты

+ доступности

– достоверности

+ целостности

7) Максимальный срок лишения свободы за создание «троянской программы»

– лишение свободы не предусмотрено

– три года

– четыре года

– пять лет

+ семь лет

– десять лет

8) Определите тип вредоносной программы, способной к самостоятельному перемещению по компьютерной сети

– компьютерный вирус

– «логическая бомба»

– троянская программа

+ компьютерный червь

9) Деятельность в сфере информационной безопасности и защиты информации на территории Российской Федерации подлежит

– сертификации

– аттестации

+ лицензированию

6.1.2. Промежуточной аттестации

Примерный перечень вопросов, выносимых на зачет

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) Регуляторы 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) Основные сущности информационной безопасности и защиты информации.
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) Классификация угроз безопасности информации.
17) Понятие компьютерной преступности: масштабы и общественная опасность.
18) Виды и субъекты компьютерных преступлений.
19) Классификация компьютерных преступлений.
20) Дисциплинарная ответственность за разглашение охраняемой законом тайны.
21) Административная ответственность за нарушения в сфере информационной безопасности и защиты информации.
22) Уголовная ответственность за преступления в сфере компьютерной информации.
23) Уголовная ответственность за нарушение закона о государственной тайне.
24) Права Регуляторов в части наложения административных взысканий за нарушения в сфере информационной безопасности и защиты информации.
25) Сфера приложения знаний специалистов по информационной безопасности и защите информации.

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.	Не зачтено

7. Ресурсное обеспечение дисциплины

7.1. Лицензионное и свободно распространяемое программное обеспечение

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

1. Astra Linux Common Edition релиз Орел - операционная систем общего назначения. Лицензия №217800111-ore-2.12-client-6196.
2. Astra Linux Special Edition - операционная система общего назначения. Лицензия №217800111-alse-1.7-client-medium-x86_64-0-14545.
3. Astra Linux Special Edition - операционная система общего назначения.Лицензия №217800111-alse-1.7-client-medium-x86_64-0-14544.

7.2. Профессиональные базы данных и информационные справочные системы

1. Портал открытых данных Российской Федерации https://data.gov.ru/ (свободный доступ).
2. Федеральный портал «Российское образование» http://www.edu.ru (свободный доступ).
3. Система официального опубликования правовых актов в электронном виде http://publication.pravo.gov.ru (свободный доступ).
4. Электронная библиотека университета http://elib.igps.ru (авторизованный доступ).
5. Электронно-библиотечная система «ЭБС» IPR BOOKS» http://www.iprbookshop.ru (авторизованный доступ).
6. 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: доктор технических наук, профессор Буйневич Михаил Викторович, кандидат технических наук, доцент Максимов Александр Викторович.