

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Горбунов Алексей Александрович

Должность: Заместитель ректора ФГБОУ ВО «Санкт-Петербургский университет ГПС МЧС России»

Дата подписания: 12.07.2024 12:04:43

Уникальный программный ключ:

286e49ee1471d400cc1f45539d51ed7bbf0e9cc7

ФГБОУ ВО «Санкт-Петербургский университет ГПС МЧС России»

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ**

Специалитет по специальности

10.05.03 – Информационная безопасность автоматизированных систем

Специализация «Анализ безопасности информационных систем»

1. Цели и задачи дисциплины

Цель освоения дисциплины:

формирование у обучающихся нового мышления, основанного на использовании новейших информационных и информационно-телекоммуникационных технологий, которые активно способствуют развитию экономики, политики, государства на основе становления информационного общества и принципах современного информационного права России; а также представления об информационных отношениях; субъектах информационно-правовых отношений; о правовом режиме получения, передачи, хранения и использования информации; о юридических аспектах информационного обмена, ответственности в информационной сфере.

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

Задачи дисциплины:

- получение знаний правовых и нормативных актов в сфере профессиональной деятельности;
- определение теоретических, концептуальных, методологических и организационных основ государственной системы защиты информации.

2. Перечень планируемых результатов обучения по дисциплине, 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, стандарты и методические документы в области защиты информации Умеет применять на практике основные нормативные правовые акты, стандарты и методические документы в области защиты информации и информационной безопасности
ОПК-5.3. Демонстрирует навыки работы с	Умеет применять на практике нормативные

нормативными документами, государственными и международными стандартами в области информационной безопасности и защиты информации	документе, государственные стандарты в области информационной безопасности и защиты информации
ОПК-6.1. Понимает меры защиты информации ограниченного доступа в автоматизированных системах; содержание нормативных правовых актов, нормативных и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Знает методологию защиты информации ограниченного доступа в автоматизированных системах согласно нормативных и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
ОПК-6.2. Определяет меры для организации защиты информации ограниченного доступа в автоматизированных системах и разрабатывает организационно-распорядительные документы, регламентирующие 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	Знает методику разработки организационно-распорядительных документов, регламентирующие защиту информации ограниченного доступа в автоматизированных системах в соответствии с действующими государственными нормативно-правовыми актами Умеет организовать и определять действия требуемые для защиты информации ограниченного доступа в автоматизированных системах
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	Умеет применять и руководствоваться на практике нормативными документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в вопросах защиты информации ограниченного доступа в автоматизированных системах

3. Место дисциплины в структуре ОПОП

Дисциплина «Государственная система защиты информации» 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 «Государственная система защиты информации» реализуется:

Для очной формы обучения в рамках обязательной части образовательной программы в объеме 108 академических часов (3 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
			9
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			+

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 и	Контроль	
9 семестр						
Раздел 1. Правовые аспекты защиты информации	54	10	16			28
Раздел 2. Защита информации в компьютерных системах	54	10	18			26
Зачет					+	
Всего за 9 семестр	108	20	34			54

4.3 Содержание дисциплины для очной формы обучения в 9 семестре:

Раздел 1. Правовые аспекты защиты информации.

Тема 1. Законодательство РФ в области информационной безопасности.

Лекции. Основные этапы развития российского законодательства об информации, информатизации и защите информации. Конституция РФ, уголовное, административное, гражданское законодательство, федеральные законы и иные нормативные акты.

Практические занятия. Правовое обеспечение безопасности информации в форме сведений и сообщений. Проблемы правового обеспечения и защиты информации в современной России. Перспективы развития законодательства в области информационной безопасности.

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 2. Государственная система защиты информации.

Лекции. Организация работ по защите информации. Структура и основные функции государственной системы защиты информации. Государственные органы управления в области информационной безопасности, их права и обязанности.

Практические занятия. Формирование информационных ресурсов и их квалификация. Конституционные гарантии прав на информацию и механизм их реализации. Информационная сфера и информационная среда. Информационная инфраструктура.

Самостоятельная работа. Структура информационной сферы и характеристика её элементов.

Рекомендуемая литература:

основная [1, 2];

дополнительная [1,2,3]

Тема 3. Лицензирование и сертификация в информационной сфере.

Лекции. Правовая основа лицензирования и сертификации в области защиты информации, в том числе государственной тайны. Виды деятельности в информационной сфере, подлежащие лицензированию.

Лицензирование деятельности по защите информации. Объекты лицензирования в сфере защиты информации. Участники лицензионных отношений в сфере защиты информации.

Практические занятия. Контроль за соблюдением лицензиатами условий ведения деятельности. Понятие сертификации по российскому законодательству. Цели и принципы сертификации. Правовая регламентация сертификационной деятельности в области защиты информации. Режимы сертификации.

Самостоятельная работа. Специальные экспертизы и государственная аттестация руководителей. Органы лицензирования и их полномочия.

Рекомендуемая литература:

основная [1, 2];

дополнительная [1,2,3]

Раздел 2. Защита информации в компьютерных системах.

Тема 4. Защита информации в компьютерных системах.

Лекции. Защита информации от потери и разрушения. Защита информации от несанкционированного доступа. Пути не санкционированного доступа. Организационные меры защиты информации. Регламентация процесса информационного обмена со сторонними организациями.

Практические занятия. Состав и организационная структура системы обеспечения информационной безопасности. Регламентация процессов и действий персонала. Обязанности сотрудников по обеспечению информационной безопасности. Регламентация процесса авторизации.

Самостоятельная работа. Регламентация применения средств защиты информации. Регламентация действий в нештатных ситуациях. Определение требований к защищенности ресурсов.

Рекомендуемая литература:

основная [1, 2];

дополнительная [1,2,3]

Рекомендуемая литература:

основная: [1,2];

дополнительная: [1,2,3]

5. Методические рекомендации по организации изучения дисциплины «Государственная система защиты информации»

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 (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 «Государственная система защиты информации»

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 – Государственная система защиты информации 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 относятся:

+ 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-компаний

- 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	Зачтено

		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.	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 «Государственная система защиты информации»

7.1. Лицензионное и свободно распространяемое программное обеспечение

Перечень лицензионного и свободно распространяемого программного обеспечения:

- 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. Метельков А.Н. Защита служебной информации в территориальных органах МЧС России криптографическими средствами: учебное пособие. МЧС России. – СПб.: СПбУ ГПС МЧС России, 2022. – 184 с. - <http://elib.igps.ru/?9&type=card&cid=ALSFR-c88b5cba-d40e-4a34-bf2c-53b6caed6a42&remote=false>

2. Метельков А.Н., Уткин О.В. Организационно-правовые и технические основы защиты конфиденциальной информации в МЧС России: учебное пособие. – СПб.: СПбУ ГПС МЧС России, 2022. – 216 с. - <http://elib.igps.ru/?10&type=card&cid=ALSFR-5db13d78-75cf-449f-8f61-04f06a5e0dd7&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

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: к.т.н., доцент Петров В.Г.