ФГБОУ ВО «Санкт-Петербургский университет ГПС МЧС России»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

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:

– состоит в формировании международных законодательных актов и договоров о защите персональных данных, Федерального законодательства России в области защиты персональных данных.

Перечень компетенций, формируемых в процессе изучения дисциплины

Компетенции	Содержание
ПК - 6	Способен разрабатывать проектные решения по защите информации в автоматизированных системах

Задачи дисциплины:

– построение частной модели угроз обработки персональных данных;

– изучить нормативные правовые акты Российской Федерации в области защиты персональных данных;

– -разрабатывать частное техническое задание на систему защиты информационной системы обработки персональных данных.

2. Перечень планируемых результатов обучения дисциплины, соотнесенных с планируемыми результатами освоения образовательной программы

Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
Применяет правила лицензирования и сертификации в области защиты информации; международные законодательные акты и договоры о защите персональных данных; Федеральное законодательство России в области защиты персональных данных ПК-6.1.	Знает
	Правовые основы защиты информации, нормативные правовые акты Российской Федерации в области персональных данных
	Умеет
	Использовать правовые основы защиты информации, нормативные правовые акты Российской Федерации в области персональных данных
Демонстрирует способности построения частной модели угроз для информационной системы обработки персональных данных; классификации информационной системы обработки персональных данных ПК-6.2.	Знает
	Особенности защиты персональных данных от несанкционированного доступа при использовании современных информационных технологий
	Умеет
	Анализировать угрозы безопасности персональных данных; определять требования к средствам защиты персональных данных
Разрабатывает частное техническое задание на систему защиты информационной	Знает
	Порядок оформления технической

системы обработки персональных данных ПК-6.3.	документации по защите персональных данных
	Умеет
	Осуществлять проверку выполнения требований нормативных, организационно-распорядительных документов по защите персональных данных
	Владеет
	Навыками разработки необходимых организационно-распорядительных документов в интересах организации по защите персональных данных

3. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Защита персональных данных» относится к части, формируемой участниками образовательных отношений 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 4 зачётные единицы, 144 часа.

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

Вид учебной работы	Трудоемкость		
	з.е.	час.	по семестрам
			8
Общая трудоемкость дисциплины по учебному плану	**4**	**144**	**144**
Контактная работа		**56**	**56**
Лекции		14	14
Практические занятия		40	40
Консультация		2	2
Самостоятельная работа		**52**	**52**
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	Консультации	Контроль	
8 семестр						
Тема 1. Актуальность защиты персональных данных	24	4	8			12
Тема 2. Угрозы безопасности персональным данным	22	2	8			12
Тема 3. Нормативная база и стандарты в области персональных данных	16	4				12
Тема 4. Организационно-технические основы администрирования и выполнения мероприятий по технической защите персональных данных	22	2	12			8
Тема 5. Создание системы обработки персональных данных	22	2	12			8
Консультация	2			2		
Экзамен	36				36	
Итого за 8 семестр	**144**	**14**	**40**	**2**	**36**	**52**

4.3 Содержание дисциплины для очной формы обучения

Тема 1. Актуальность защиты персональных данных

Лекции. Актуальность вопросов защиты персональных данных и мировые тенденции по защите персональных данных. Международные законодательные акты в области защит персональных данных Федеральное законодательство в области защиты персональных данных. Техническая защита персональных данных. Разработка частной модели угроз.

Практические занятия.

Оценка актуальности угроз обработки персональных данных. Разработка частной модели угроз.

Самостоятельная работа.

Предварительные работы по защите персональных данных.

Рекомендуемая литература:

Основная литература: [1, 2];

Дополнительная литература:[1,2]

Тема 2. Угрозы безопасности персональным данным.

Лекция. Угрозы безопасности персональным данным. Модели угроз безопасности персональным данным.

Банк данных угроз безопасности персональным данным, включающий базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах.

Практические занятия.

Методы выявления и анализа угроз безопасности персональным данным, уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах.

Самостоятельная работа.

Информационные ресурсы, государственные информационные ресурсы, находящиеся в ведении органов государственной власти.

Рекомендуемая литература:

Основная литература: [1,2];

Дополнительная литература:[1,2].

Тема 3. Нормативная база и стандарты в области персональных данных и технической защиты информации.

Лекция. Правовые основы защиты информации. Нормативные правовые акты Российской Федерации. Нормативные правовые акты и документы ФСТЭК России. Нормативные правовые акты МЧС России.

Самостоятельная работа.

Система документов в области обеспечения безопасности персональных данных.

Рекомендуемая литература:

Основная литература: [1,2];

Дополнительная литература:[1,2].

Тема 4. Организационно-технические основы администрирования и выполнения мероприятий по технической защите персональных данных

Лекция. Комплекс мероприятий по защите персональных данных. Особенности защиты информации от несанкционированного доступа при использовании современных информационных технологий (мобильных, беспроводных, суперкомпьютерных, виртуализации, облачных, больших данных и др.)

Практические занятия.

Установка и работа с средствами доверенной загрузки. Настройка штатных средств защиты информации в операционной системе.

Самостоятельная работа.

Системные и документальные части системы защиты информации от несанкционированного доступа.

Рекомендуемая литература:

Основная литература: [1,2];

Дополнительная литература: [1,2]

Тема 5. Создание системы обработки персональных данных

Лекция. Разработка Технического задания на информационную систему обработки персональных данных. Разработка Частного технического задания на систему защиты системы обработки персональных данных. Выбор средств защиты информации. Аттестация объектов информатизации и защищаемых помещений для обработки персональных данных.

Практические занятия.

Разбор инцидентов в информационных системах обработки персональных данных. Создание системы обработки персональных данных.

Самостоятельная работа.

Запуск в промышленную эксплуатацию информационных систем обработки персональных данных. Регламентные работы в информационных системах обработки персональных данных

Рекомендуемая литература:

Основная литература:: [1,2];

Дополнительная литература: [1,2]

5. Методические рекомендации по организации изучения дисциплины

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

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

Промежуточная аттестация обеспечивает оценивание промежуточных и окончательных результатов обучения по дисциплине, проводится в форме экзамена.

6.1. Примерные оценочные материалы:

6.1.1. Текущего контроля

Типовые вопросы для опроса:

1. Сколько уровней защищенности персональных данных устанавливается при обработке персональных данных в информационных системах ;
2. На какой федеральный орган исполнительной власти возложена обязанность по осуществлению контроля и надзора за обработкой персональных данных ;
3. Фотографические изображения обучающихся, сотрудников и посетителей организации относят ;
4. Дайте определение основным терминам системы паролирования (идентификации, аутентификации и авторизации);
5. Перечислите основные типы атак на систему паролирования;
6. Назовите признаки «идеального» пароля;
7. Перечислите структурные элементы системы контроля и управления доступом;
8. Перечислите структурные элементы системы охраны периметра;
9. Оператор персональных данных - это;
10. Назовите масштабы компьютерной преступности;
11. Приведите структуру кодификатора Интерпола;
12. Раскройте специфику расследования компьютерных преступлений.
13. Назовите виды ответственности за нарушения в сфере информационной безопасности и защиты информации;
14. Перечислите статьи Уголовного кодекса РФ в части ответственности за преступления в сфере компьютерной информации;
15. Назовите статью Уголовного кодекса РФ, регламентирующую ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации.

16. Приведите права регуляторов в части наложения административных взысканий за нарушения в сфере информационной безопасности и защиты информации

17. История компьютерных вирусов

18. Классификация вирусов

19. Признаки присутствия на компьютере вредоносных программ

20. Методы обнаружения подозрительных файлов.

Типовые задания для тестирования:

1. Сколько уровней защищенности персональных данных устанавливается при обработке персональных данных в информационных системах?

1) Три
2) Четыре
3) Пять
4) Шесть

2. Каким нормативным правовым актом устанавливаются требования к защите персональных данных при их обработке в информационных системах персональных данных

1) ФЗ № 152 от 27.07.2006
2) Указом Президента Российской Федерации № 188 от 06.03.1997 г.
3) Постановлением Правительства Российской Федерации от 01 ноября 2012 г. N 1119
4) ФЗ № 149 от 27.07.2006

3. На какой федеральный орган исполнительной власти возложена обязанность по осуществлению контроля и надзора за обработкой персональных данных

1) ФСТЭК России
2) ФСБ России
3) МВД России
4) Роскомнадзор

4. Какой срок действия лицензии на деятельность по технической защите конфиденциальной информации

1) 3 года
2) 5 лет
3) 10 лет
4) бессрочно

5. Какой максимальный срок действия сертификата на средства защиты информации:

1) 3 года

2) 5 лет
3) 10 лет
4) бессрочно

6. Сколько классов защищенности СВТ от НСД устанавливается в РД ФСТЭК «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации»:
1) 4
2) 5
3) 6
4) 8

7. Механизм защиты входа пользователя в систему реализуется в составе:
1) подсистемы управления доступом
2) подсистемы регистрации и учета (аудита)
3) подсистемы обеспечения целостности
4) криптографической подсистемы

8. Какие федеральные органы исполнительной власти осуществляют разработку требований к методам и средствам защиты информации в АС:
1) ФСТЭК России;
2) МВД России
3) Роскомнадзор
4) МЧС России

9. Какую информацию запрещено относить к конфиденциальной в соответствии с законом РФ?
1) Паспортные данные гражданина
2) Информация, накапливаемая в открытых фондах библиотек, музеев, архивов
3) Себестоимость продукта и объем сбыта
4) Контактные данные клиентов

10. Какие действия можно производить с персональными данными?
1) чтение и рассылка
2) хранение, уничтожение
3) обезличивание, блокирование
4) фасовка и упаковка.

Примерный перечень вопросов выносимых на экзамен

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. Действия, выполняемые компонентами в процессе работы
14. Основы работы антивирусных программ
15. Дополнительные средства обеспечения антивирусной безопасности Основные элементы антивирусной защиты
16. Критерии выбора антивирусных продуктов для обеспечения эффективной защиты компьютера от проникновения вирусов
17. Назначение и принципы действия программ, необходимых для полноценной и эффективной защиты компьютеров от вредоносного воздействия
18. Принципы построения и управления системой антивирусной защиты локальных сетей
19. Угрозы заражения мобильных пользователей
20. Принципы действия вирусов для мобильных телефонов
21. Средства защиты от вирусов мобильных систем
22. Антивирусная защита компьютерных систем
23. Принципы построения системой антивирусной защиты компьютерных систем
24. Управление системой антивирусной защиты компьютерных систем
25. Администрирование КС (АС)
26. Органы управления и планирования эксплуатации защищенных АС
27. Эксплуатационная документация на АС (изделия ИТ).
28. Руководства пользователя и администратора

29. Конструкторские эксплуатационные документы на ТСО и ПО, эксплуатационные документы предприятия

30. Работа алгоритма Алоха в канале с ложными конфликтами.

31. Соответствие между IP и MAC-адресами.

32. Транспортный уровень. UDP-протокол.

6.2. Шкала оценивания результатов промежуточной аттестации и критерии выставления оценок

Система оценивания включает:

Форма контроля	Показатели оценивания	Критерии выставления оценок	Шкала оценивания
экзамен	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.

7.1. Лицензионное и свободно распространяемое программное обеспечение

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

1. Лицензия №217800111-ore-2.12-client-6196

Выдана «ФГБОУ ВО Санкт-Петербургский университет ГПС МЧС России» на право использования: Astra Linux Common Edition релиз Орел

Срок действия: бессрочно

2. Лицензия №217800111-alse-1.7-client-medium-x86_64-0-14545

Выдана «ФГБОУ ВО Санкт-Петербургский университет ГПС МЧС России» на право использования: Astra Linux Special Edition

Срок действия: бессрочно

3. Лицензия №217800111-alse-1.7-client-medium-x86_64-0-14544

Выдана «ФГБОУ ВО Санкт-Петербургский университет ГПС МЧС России» на право использования Astra Linux Special Edition

Срок действия: бессрочно

4. ПО «Р7-Офис. Профессиональный»

Выдана: «ФГБОУ ВО Санкт-Петербургский университет МЧС России»

Срок действия: бессрочно

7.2. Профессиональные базы данных и информационные справочные системы

1. Сервер органов государственной власти Российской Федерации http://россия.рф/ (свободный доступ);
2. Портал открытых данных Российской Федерации https://data.gov.ru/ (свободный доступ);
3. Федеральный портал «Российское образование» http://www.edu.ru (свободный доступ);
4. Система официального опубликования правовых актов в электронном виде http://publication.pravo.gov.ru (свободный доступ);
5. Федеральный портал «Совершенствование государственного управления» https://ar.gov.ru (свободный доступ);
6. Электронная библиотека университета http://elib.igps.ru (авторизованный доступ);
7. Электронно-библиотечная система «ЭБС IPR BOOKS» http://www.iprbookshop.ru (авторизованный доступ).
8. Электроно-библиотечная система "Лань" https://e.lanbook.com (авторизованный доступ).

7.3. Литература

Основная литература:

1. Организационно-правовые и технические основы защиты конфиденциальной информации в МЧС России: учебное пособие: [гриф МЧС] / А.Н. Метельков, О.В. Уткин О.В.; – СПб.: СПбУ ГПС МЧС России, 2022. – 216 с. Режим доступа: https://elib.igps.ru/?6&type=card&cid=ALSFR-5db13d78-75cf-449f-8f61-04f06a5e0dd7&remote=false

2. Защита служебной информации в территориальных органах МЧС России криптографическими средствами : учебное пособие / А.Н. Метельков – СПб.: СПбУ ГПС МЧС России, 2022. – 184 с. Режим доступа: https://elib.igps.ru/?5&type=card&cid=ALSFR-c88b5cba-d40e-4a34-bf2c-53b6caed6a42&remote=false

Дополнительная 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. Информационная безопасность : учебное пособие / В. И. Лойко, В. Н. Лаптев, Г. А. Аршинов, С. Н. Лаптев. — Краснодар : КубГАУ, 2020. — 332 с. — ISBN 978-5-907346-50-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/254168 (дата обращения: 28.02.2025). — Режим доступа: для авториз. пользователей.

7.4. Материально-техническое обеспечение

Для проведения и обеспечения занятий используются помещения, которые представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой, оснащенные оборудованием и техническими средствами обучения: автоматизированное рабочее место преподавателя, маркерная доска, интерактивная доска, мультимедийный проектор, документ-камера, посадочные места обучающихся.

Помещения для практических занятий и самостоятельной работы обучающихся оснащены компьютерной техникой, с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде университета.

Автор: кандидат юридических наук Метельков Александр Николаевич.