

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

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 изучении 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
Проектный тип деятельности	
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
Демонстрирует способности построения частной модели угроз для информационной системы обработки персональных данных; классификации информационной системы обработки персональных данных ПК-6.2.	Умеет
	Использовать правовые основы защиты информации, нормативные правовые акты Российской Федерации в области персональных данных
	Знает
Умеет	Особенности защиты персональных данных от несанкционированного доступа при использовании современных информационных технологий
	Анализировать угрозы безопасности персональных данных; определять требования к средствам защиты персональных данных

Разрабатывает частное техническое задание на систему защиты информационной системы обработки персональных данных ПК-6.3.	Знает
	Порядок оформления технической 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 ОПОП

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

Дисциплина «Защита персональных данных» реализуется:

Для очной формы обучения в рамках части образовательной программы в объеме 144 академических часов (4 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
			8
Общая трудоемкость дисциплины по учебному плану	4	144	144
Контактная работа, в том числе:		56	56
Аудиторные занятия		54	54
Лекции (Л)		14	14
Практические занятия (ПЗ)		40	40
Консультация		2	2
Самостоятельная работа (СРС)		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 и	Контроль	
8 семестр						
Актуальность защиты персональных данных	24	4	8			12
Угрозы безопасности персональным данным	22	2	8			12
Нормативная база и стандарты в области персональных данных	16	4				12
Организационно-технические основы администрирования и выполнения мероприятий по технической защите персональных данных	22	2	12			8
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

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

Практическое занятие.

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

Самостоятельная работа.

Предварительные работы по защите персональных данных.

Рекомендуемая литература:

основная [1, 2];

дополнительная [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.

Практическое занятие.

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 [1,2];

дополнительная [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 [1,2];

дополнительная [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, грид, суперкомпьютерных, виртуализации, облачных, больших данных и др.)

Практическое занятие.

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 [1,2];

дополнительная [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.

Практическое занятие.

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: [1,2];

дополнительная: [1,2]

5. Методические рекомендации по организации изучения дисциплины «Защита персональных данных»

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 «Защита персональных данных»

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.

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

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 «Защита персональных данных»

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

Информационная справочная система — Сервер органов государственной власти Российской Федерации <http://россия.рф/> (свободный доступ); профессиональные базы данных — Портал открытых данных Российской Федерации <https://data.gov.ru/> (свободный доступ); федеральный портал «Российское образование» <http://www.edu.ru> (свободный доступ); система официального опубликования правовых актов в электронном виде <http://publication.pravo.gov.ru/> (свободный доступ); федеральный портал «Совершенствование государственного управления» <https://ar.gov.ru> (свободный доступ); электронная библиотека университета <http://elib.igps.ru> (авторизованный доступ); электронно-библиотечная система «ЭБС IPR BOOKS» <http://www.iprbookshop.ru> (авторизованный доступ)

7.3. Литература

Основная литература:

1. Безопасность информационных систем и защита информации в МЧС России: учебное пособие: [гриф МЧС] / Ю.И. Синешук [и др.]; ред. В.С. Артамонов; С.-Петербург. 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. Организационно-правовое обеспечение информационной безопасности : учеб. пособие для вузов / Стрельцов А. А., Горбатов В. С., Полякова Т. А. [и др.] ; ред. Стрельцов А. А. - М. : Академия, 2008. - 248 с. - (Высшее профессиональное образование. Информационная безопасность). - Библиогр.: с. 242-245. - ISBN 978-5-7695-4240-4

Дополнительная литература:

1. Основы информационной безопасности: учеб. пособие для вузов / Акулов О. А., Баданин Д. Н., Жук Е. И. [и др.]; МГТУ им. Н. Э. Баумана. - М.: Изд-во МГТУ им. Н. Э. Баумана, 2008. - 159 с. - Библиогр.: с. 157-158. - ISBN 978-5-7038-3211-0

2. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс]: учеб. Пособие. — Электрон. дан. — Москва: ДМКПресс, 2014.—702с.— Режим доступа: <https://e.lanbook.com/book/50578>.

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 из расчета 1 компьютер на одного обучающегося, с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде университета.

Авторы: к.ю.н., Метельков А.Н.