Министерство науки и высшего образования Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Санкт-Петербургский государственный университет промышленных технологий и дизайна»
(СПбГУПТД)

УТВЕРЖДАЮ
Директор ВШТЭ

Рабочая программа дисциплины

Б1.В.04 Хранение и защита компьютерной информации в АСУ

Учебный план: ФГОС3++zm150404-1_21_13.plx

Кафедра: 1 Информационно-измерительных технологий и систем управления

Направление подготовки: (специальность) 15.04.04 Автоматизация технологических процессов и производств

Профиль подготовки: (специализация) Системы автоматизации и управления технологическими процессами

Уровень образования: магистратура

Форма обучения: заочная

План учебного процесса

Семестр (курс для ЗАО)		Контактная работа обучающихся		Сам. работа	Контроль, час.	Трудоёмкость, ЗЕТ	Форма промежуточной аттестации
		Лекции	Лаб. занятия				
2	УП	4	8	56	4	2	Зачет
	РПД	4	8	56	4	2	
Итого	УП	4	8	56	4	2	
	РПД	4	8	56	4	2	

Санкт-Петербург
2021

Рабочая программа дисциплины составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 15.04.04 Автоматизация технологических процессов и производств, утверждённым приказом Министерства образования и науки Российской Федерации от 25.11.2020 г. № 1452

Составитель (и):

Кандидат технических наук, доцент — Морева С.Л.

От кафедры составителя: — Сидельников В.И.
Заведующий кафедрой информационно-измерительных технологий и систем управления

От выпускающей кафедры: — Сидельников В.И.
Заведующий кафедрой

Методический отдел: — Смирнова В.Г.

1 ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1 Цель дисциплины: Целью дисциплины является формирование у студентов знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных средств в автоматизированных системах управления.

1.2 Задачи дисциплины:

Рассмотреть модели и методы представления и хранения информации;

Рассмотреть существующие угрозы безопасности информации в АСУ;

Раскрыть принципы и методы подбора и применения современных методов и способов защиты информации;

Приобрести практические навыки обеспечения защиты информации и применения программно-технических мер обеспечения компьютерной безопасности в АСУ.

1.3 Требования к предварительной подготовке обучающегося:

Предварительная подготовка предполагает создание основы для формирования компетенций, указанных в п. 2, при изучении дисциплин:

Метрологическое и информационное обеспечение систем автоматизации и управления

Современные проблемы автоматизации и управления

2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-5: Способен осуществлять контроль разработки и управление разработкой АСУП в своей профессиональной деятельности
Знать: основы обеспечения информационной безопасности, методы и средства защиты информации; стандарты информационной безопасности и защиты хранимых и передаваемых данных.
Уметь: использовать прикладные программы управления проектами для планирования и контроля выполнения мероприятий по защите и обеспечению надежности хранения данных АСУП и АСУТП.
Владеть: навыками планирования и контроля выполнения мероприятий по защите и обеспечению надежности хранения данных АСУП и АСУТП.

3 РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Наименование и содержание разделов, тем и учебных занятий	Семестр (курс для ЗАО)	Контактная работа		СР (часы)	Инновац. формы занятий
		Лек. (часы)	Лаб. (часы)		
Раздел 1. Хранение информации	2				
Тема 1. Основные понятия информационной безопасности. Информация, данные, знания. Типы структур, модели данных. Операции над данными. Ограничения целостности. Администрирование базы данных. Механизмы среды хранения и архитектура БД. Структура хранимых данных. Управление пространством памяти и размещением данных. Виды адресации хранимых записей. Способы размещения данных и доступа к данным в БД. Лабораторная работа 1. Механизмы среды хранения и архитектура БД. Способы размещения данных и доступа к данным в БД.		0,5	1	11	
Тема 2. Хранение, доступ и защита данных в базах данных. Угрозы безопасности БД: общие и специфические. Требования безопасности БД. Защита от несанкционированного доступа (НСД). Защита от вывода. Целостность БД. Аудит. Задачи и средства администратора безопасности баз данных. Многоуровневая защита. Лабораторная работа 2. Угрозы безопасности БД и защита от них.		0,5	1	11	
Раздел 2. Защита информации в АСУ					
Тема 3. Основные понятия и угрозы информационной безопасности. Основные составляющие ИБ. Важность и сложность проблемы ИБ. Наиболее распространенные угрозы ИБ. Наиболее распространенные угрозы доступности, конфиденциальности, целостности. Вредоносное программное обеспечение. Основные правила защиты от "компьютерных вирусов". Обзор и методика использования антивирусных программ. Восстановление пораженных "компьютерными вирусами" объектов. Лабораторная работа 3. Основные составляющие информационной безопасности. Угрозы ИБ. Обзор и методика использования антивирусных программ.		1	2	11	

Тема 4. Основы законодательства в области информационной безопасности. Обзор российского законодательства в области информационной безопасности. Обзор зарубежного законодательства в области информационной безопасности. Текущее состояние российского законодательства в области информационной безопасности. Стандарты и спецификации в области информационной безопасности. Лабораторная работа 4. Изучение международных стандартов в области информационной безопасности.		1	2	11	
Тема 5. Программно-технические меры обеспечения компьютерной безопасности в АСУ. Основные понятия программно-технического уровня информационной безопасности. Идентификация и аутентификация, управление доступом. Парольная аутентификация. Одноразовые пароли. Применение биометрических систем идентификации. Протоколирование и аудит, шифрование, контроль целостности. Методы криптографического шифрования. Экранирование. Архитектурные аспекты. Классификация межсетевых экранов. Анализ защищенности. Обеспечение высокой доступности. Отказоустойчивость и зона риска. Программное обеспечение промежуточного слоя. Обеспечение отказоустойчивости и обслуживаемости. Лабораторная работа 5. Программно-технические меры обеспечения компьютерной безопасности информационных систем. Идентификация и аутентификация, управление доступом.		1	2	12	
Итого в семестре (на курсе для ЗАО)		4	8	56	
Консультации и промежуточная аттестация (Зачет)		0,25			
Всего контактная работа и СР по дисциплине		12,25		56	

4 КУРСОВОЕ ПРОЕКТИРОВАНИЕ

Курсовое проектирование учебным планом не предусмотрено

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

5.1 Описание показателей, критериев и системы оценивания результатов обучения

5.1.1 Показатели оценивания

Код компетенции	Показатели оценивания результатов обучения	Наименование оценочного средства
ПК-5	1. Имеет представление о нормативно-правовых документах в области информационной безопасности и об ответственности в этой сфере, о методах и средствах защиты информации. 2. Демонстрирует применение современных программно-технических методов и средств защиты от угроз безопасности информации в автоматизированных системах управления.	1. Вопросы устного собеседования. 2. Практико-ориентированные задания 3.Тестовые задания.

	3. Демонстрирует навыки по обеспечению безопасности информации в автоматизированных системах управления для решения практических задач по защите и обеспечению надежности хранения данных.	

5.1.2 Система и критерии оценивания

Шкала оценивания	Критерии оценивания сформированности компетенций	
	Устное собеседование	Письменная работа
Зачтено	Обучающийся свободно ориентируется в основных понятиях и терминах по защите информации; усвоил основную и знаком с дополнительной литературой по обеспечению информационной безопасности, возможно допустил несущественные ошибки в ответе на вопросы преподавателя.	Обучающийся своевременно выполнил тестовое задание, решил типовые задачи.
Не зачтено	Обучающийся неспособен сформулировать хотя бы отдельные концепции по защите информации, допустил существенные ошибки в ответе на вопросы преподавателя. Попытка списывания, использования неразрешенных технических устройств или пользование подсказкой другого человека.	Обучающийся не выполнил тестовое задание, не решил типовые задачи.

5.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности

5.2.1 Перечень контрольных вопросов

№ п/п	Формулировки вопросов
	Курс 2
1	Дайте определение понятиям «Управление доступом, ограничение, разграничение, разделение доступа к информации» и сформулируйте их основные характеристики.
2	Сформулируйте преимущества и недостатки метода криптографического преобразования информации.
3	Сформулируйте понятия и дайте характеристику «аутентификация пользователей», «парольная аутентификация».
4	Сформулируйте понятие «Идентификация пользователей». Классификация методов идентификации пользователей.
5	Назовите мероприятия по защите информации от несанкционированного доступа.
6	Классификация технических средств защиты информации.
7	Какие вы знаете современные технические средства защиты информации.
8	Назовите способы защиты информации от утечки по техническим каналам.
9	Сформулируйте понятие «утечка данных». Назовите каналы утечки и нарушения безопасности компьютерной информации.
10	Сформулируйте текущее состояние российского законодательства в области информационной безопасности.
11	Сформулируйте понятие законодательного уровня информационной безопасности.
12	Назовите признаки заражения компьютера вредоносной программой.
13	Сформулируйте достоинства и недостатки современных антивирусных программ.
14	Сформулируйте понятие «Вредоносные программы (вирусы)». Классификация компьютерных вирусов.
15	Сформулируйте виды противников или «нарушителей» информационной безопасности.
16	Назовите виды атак и методы взлома информационных сетей злоумышленниками.
17	Назовите наиболее распространенные пути и каналы утечки информации.
18	Назовите наиболее распространенные угрозы для компьютерной информации в АСУ.
19	Угрозы безопасности БД и защита от них.
20	Способы размещения данных и доступа к данным в БД.
21	Администрирование базы данных.
22	Механизмы среды хранения и архитектура БД.
23	Операции над данными. Ограничения целостности.
24	Сформулируйте понятия «доступность», «целостность», «конфиденциальность информации».

25	Какие Вы знаете категории и носители информации.
26	Назовите объекты защиты при обеспечении компьютерной безопасности.
27	Определите понятия «безопасность информации» и его отличие от понятия «защита информации».
28	Сформулируйте понятия и основные составляющие информационной безопасности.

5.2.2 Типовые тестовые задания

Потенциальные угрозы, против которых направлены технические меры защиты информации:

а) потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей

б) потери информации из-за не достаточной установки сигнализации в помещении

в) потери информации из-за халатности обслуживающего персонала и не ведения системы наблюдения

Для защиты от злоумышленников необходимо использовать:

а) системное программное обеспечение

б) прикладное программное обеспечение

в) антивирусные программы

Что является наиболее надежным средством предотвращения потерь компьютерной информации при кратковременном отключении электроэнергии?

а) установка источников бесперебойного питания

б) такого средства не существует

в) перекидывать информацию на носитель, который не зависит от энергии

Программные средства защиты можно разделить на:

а) правовые, аппаратные, программные

б) административные меры защиты, включающие подготовку и обучение персонала, организацию тестирования и приема в эксплуатацию программ, контроль доступа в помещения и т.д.

в) криптография, антивирусные программы, системы разграничения полномочий, средства контроля доступа и т.д.

5.2.3 Типовые практико-ориентированные задания (задачи, кейсы)

1. Вы – начальник отдела по вопросам информационной безопасности в некоторой не крупной организации (20-30 человек).

Вам необходимо разработать требования к хранению, использованию и утилизации информации для Вашей организации.

Цель: обеспечение информационной безопасности, при хранении, обработке, передаче и уничтожении информации.

2. Проработайте требования для специалистов по подбору кадров Вашей организации, с целью внесения пунктов об информационной безопасности в трудовой договор новых сотрудников.

Цель: уведомление новых сотрудников о строгом выполнении требований по обеспечению информационной безопасности и ответственности за их нарушение.

3. Придумать символьный пароль, преобразовать его в ключ и зашифровать (и расшифровать) фразу открытого текста с помощью этого ключа.

5.3 Методические материалы, определяющие процедуры оценивания знаний, умений, владений (навыков и (или) практического опыта деятельности)

5.3.1 Условия допуска обучающегося к промежуточной аттестации и порядок ликвидации академической задолженности

Проведение промежуточной аттестации регламентировано локальным нормативным актом СПбГУПТД «Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся»

5.3.2 Форма проведения промежуточной аттестации по дисциплине

Устная	×	Письменная	×	Компьютерное тестирование		Иная	

5.3.3 Особенности проведения промежуточной аттестации по дисциплине

Возможность пользоваться конспектом лекций и записями материалов практических занятий.

Время на выполнение тестового задания – 15 минут.

Время на подготовку к устному собеседованию – 20 минут, на ответ – 10 минут.

В течение семестра выполняется одна контрольная работа.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
6.1.1 Основная учебная литература				

Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации	Москва: ИЦ РИО&#xfffd;	2021	https://ibooks.ru/reading.php?short=1&productid=361272
Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование	2019	http://www.iprbookshop.ru/87995.html
6.1.2 Дополнительная учебная литература				
Бусыгин К. Н., Васильева Е. К., Дружкина Ю. Д.	Защита информации и информационная безопасность	Санкт-Петербург: СПбГУПТД	2016	http://publish.sutd.ru/tp_ext_inf_publish.php?id=3007
Жук А.П., Жук Е.П., Лепешкин О.М. и др.	Защита информации	Москва: ИЦ РИО&#xfffd;	2021	https://ibooks.ru/reading.php?short=1&productid=361250
Никифоров, С. Н.	Защита информации. Защита от внешних вторжений	Санкт-Петербург: Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ	2017	http://www.iprbookshop.ru/74381.html
Астайкин, А. И., Мартынов, А. П., Николаев, Д. Б., Фомченко, В. Н.	Информационная безопасность и защита информации. В 2 томах. Т. 2	Саров: Российский федеральный ядерный центр – ВНИИЭФ	2017	http://www.iprbookshop.ru/89889.html

6.2 Перечень профессиональных баз данных и информационно-справочных систем

Электронно-библиотечная система IPRbooks [Электронный ресурс]. URL: http://www.iprbookshop.ru/
Электронная библиотека ВШТЭ СПБ ГУПТД [Электронный ресурс]. URL: http://nizrp.narod.ru
Электронно-библиотечная система «Айбукс» [Электронный ресурс]. URL: https://www.ibooks.ru/

6.3 Перечень лицензионного и свободно распространяемого программного обеспечения

MicrosoftWindows 8

MicrosoftOfficeProfessional 2013

6.4 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Аудитория	Оснащение
Лекционная аудитория	Мультимедийное оборудование, специализированная мебель, доска
Компьютерный класс	Мультимедийное оборудование, компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду