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.08 Защита информации в системах управления и автоматизации

Учебный план: ФГОС3++b270304-1_21-14.plx

Кафедра: 1 Информационно-измерительных технологий и систем управления

Направление подготовки: (специальность) 27.03.04 Управление в технических системах

Профиль подготовки: (специализация) Системы и средства автоматизации технологических процессов

Уровень образования: бакалавриат

Форма обучения: очная

План учебного процесса

Семестр (курс для ЗАО)		Контактная работа обучающихся		Сам. работа	Контроль, час.	Трудоёмкость, ЗЕТ	Форма промежуточной аттестации
		Лекции	Практ. занятия				
7	УП	17	34	56,75	0,25	3	Зачет
	РПД	17	34	56,75	0,25	3	
Итого	УП	17	34	56,75	0,25	3	
	РПД	17	34	56,75	0,25	3	

Санкт-Петербург
2021

Рабочая программа дисциплины составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 27.03.04 Управление в технических системах, утверждённым приказом Министерства образования и науки Российской Федерации от 31.07.2020 г. № 871

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, ознакомление студентов с тенденцией развития информационной безопасности, с моделями возможных угроз и основными нормативными документами России, по данному вопросу, формирование практических умений и навыков применения современных технологий обеспечения защиты информации в системах управления и автоматизации.

1.2 Задачи дисциплины:

• Рассмотреть существующие угрозы безопасности информации в системах управления и автоматизации;

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

• Приобрести практические навыки работы по защите информации в системах управления и автоматизации.

1.3 Требования к предварительной подготовке обучающегося:

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

Безопасность объектов автоматизации и управления

Информационные системы на базах данных в АСУ ТП

2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-6: Способен управлять защитой информации в автоматизированных системах
Знать: Нормативно-правовые основы информационной безопасности; ответственность за нарушения в сфере информационной безопасности.
Уметь: Квалифицировать нарушения и угрозы безопасности информации систем управления и автоматизации; применять нормативно-правовые документы в области защиты информации.
Владеть: навыками оценки угроз безопасности информации в системах управления и автоматизации, и последствий от их возможной реализации; терминологией в области защиты информации.

3 РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Наименование и содержание разделов, тем и учебных занятий	Семестр (курс для ЗАО)	Контактная работа		СР (часы)	Инновац. формы занятий	Форма текущего контроля
		Лек. (часы)	Пр. (часы)			
Раздел 1. Основы информационной безопасности	7					О
Тема 1. Теоретические основы информационной безопасности. Современное состояние защиты информации. Понятие, основные определения и составляющие информационной безопасности. Доступность, целостность, конфиденциальность.		1	2	4		
Тема 2. Актуальность защиты информации Важность и сложность проблемы информационной безопасности. Анализ проблематики, связанной с информационной безопасностью. Проблемы защиты информации в интернете. Ценность информации.		1	2	4		
Раздел 2. Угрозы информационной безопасности в системах управления и автоматизации						Л
Тема 3. Виды угроз. Наиболее распространенные угрозы, пути и каналы утечки информации, от кого они исходят и к чему приводят. Изучение видов атак и методов взлома интрасетей злоумышленниками. Виды возможных нарушений информационной системы. Виды противников или «нарушителей».		2	4	7		
Тема 4. Вредоносное программное обеспечение. Основные правила защиты от «компьютерных вирусов». Обзор и методика использования антивирусных программ. Восстановление пораженных «компьютерными вирусами» объектов.		2	4	7		
Раздел 3. Законодательство в области информационной безопасности						Л

Тема 5. Основы законодательства в области информационной безопасности Что такое законодательный уровень информационной безопасности и почему он важен. Обзор российского законодательства в области ИБ. Ответственность на нарушения ИБ.		2	4	8		
Тема 6. Лицензирование и сертификация в информационной безопасности Нормы и требования российского законодательства в области лицензирования и сертификации. Порядок оформления и получения лицензий и сертификатов в области ИБ.		3	6	8		
Раздел 4. Программно-технические меры обеспечения компьютерной безопасности систем управления и автоматизации						Л
Тема 7. Технические средства защиты информации в системах управления. Способы и средства защиты информации от утечки по техническим каналам. Методы и средства контроля эффективности защиты объектов информатизации, и от утечки информации по техническим каналам.		3	6	8,75		
Тема 8. Программно-технические меры защиты информации в системах управления и автоматизации. Основные понятия программно-технического уровня информационной безопасности. Рассматриваются методы защиты информации в системах управления: ограничение доступа, разграничение доступа, разделение доступа, криптографическое преобразование информации, контроль и учет доступа, законодательные меры, обеспечение информационной безопасности в Internet. Основные технологии построения защищенных ИС.		3	6	10		
Итого в семестре (на курсе для ЗАО)		17	34	56,75		
Консультации и промежуточная аттестация (Зачет)		0,25				
Всего контактная работа и СР по дисциплине		51,25		56,75		

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-6	1. Имеет представление о нормативно-правовых документах в области информационной безопасности и об ответственности в этой сфере. 2. Демонстрирует применение современных программно-технических методов и средств защиты от угроз безопасности информации в системах управления и автоматизации. 3. Использует теоретические знания по обеспечению безопасности информации в системах управления и автоматизации для решения практических задач.	1. Вопросы устного собеседования 2. Тестовые задания

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
Семестр 7	
1	Сформулируйте понятия и основные составляющие информационной безопасности
2	Определите понятия «безопасность информации» и его отличие от понятия «защита информации»
3	Назовите объекты защиты при обеспечении компьютерной безопасности
4	Какие Вы знаете категории и носители информации
5	Сформулируйте понятия «доступность», «целостность», «конфиденциальность информации»
6	Обоснуйте важность проблемы компьютерной информационной безопасности
7	Классификация информации по степени важности
8	Обоснуйте проблемы защиты информации в интернете
9	Сформулируйте понятие «ценность информации». Назовите порядковую шкалу ценностей
10	Формулировка актуальности решения проблем защиты информации
11	Назовите наиболее распространенные угрозы для компьютерной информации
12	Назовите наиболее распространенные пути и каналы утечки информации
13	Назовите виды атак и методы взлома информационных сетей злоумышленниками
14	Сформулируйте виды противников или «нарушителей» информационной безопасности
15	Назовите виды возможных нарушений информационной системы
16	Сформулируйте понятие «Вредоносные программы (вирусы)». Классификация компьютерных вирусов
17	Назовите основные правила защиты от компьютерных вирусов
18	Назовите современные антивирусные программы
19	Сформулируйте достоинства и недостатки современных антивирусных программ

20	Назовите признаки заражения компьютера от вредоносных программ
21	Сформулируйте понятие законодательного уровня информационной безопасности
22	Объясните важность законодательного уровня информационной безопасности
23	Назовите критерии безопасности компьютерных систем
24	Сформулируйте текущее состояние российского законодательства в области информационной безопасности
25	В каком случае сотрудник учреждения может быть привлечен к ответственности за нарушения правил информационной безопасности?
26	Назовите требования российского законодательства в области лицензирования и сертификации
27	Сформулируйте основные понятия в области лицензирования
28	Объясните порядок оформления и получения лицензий в области информационной безопасности
29	Сформулируйте причины отказа в получении лицензии
30	Объясните порядок оформления и получения сертификатов в области информационной безопасности
31	Сформулируйте понятие «утечка данных». Назовите каналы утечки и нарушения безопасности компьютерной информации
32	Назовите способы защиты информации от утечки по техническим каналам
33	Какие вы знаете современные технические средства защиты информации
34	Классификация технических средств защиты информации
35	Назовите мероприятия по защите информации от несанкционированного доступа
36	Назовите методы защиты информации
37	Сформулируйте понятие «Идентификация пользователей». Классификация методов идентификации пользователей
38	Сформулируйте понятия и дайте характеристику «аутентификация пользователей», «парольная аутентификация»
39	Дайте определение понятиям «Управление доступом, ограничение, разграничение, разделение доступа к информации» и сформулируйте их основные характеристики
40	Сформулируйте преимущества и недостатки метода криптографического преобразования информации

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)

Не предусмотрено

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.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
6.1.1 Основная учебная литература				
Запонов, Э. В., Мартынов, А. П., Машин, И. Г., Николаев, Д. Б., Сплюхин, Д. В., Фомченко, В. Н.	Методы и средства комплексной защиты информации в технических системах	Саров: Российский федеральный ядерный центр – ВНИИЭФ	2019	http://www.iprbookshop.ru/101925.html
Фомин, Д. В.	Информационная безопасность	Саратов: Вузовское образование	2018	http://www.iprbookshop.ru/77319.html
Евстифеев, А. А., Ерошев, В. И., Мартынов, А. П., Николаев, Д. Б., Сплюхин, Д. В., Фомченко, В. Н.	Основы защиты информации от утечки по техническим каналам	Саров: Российский федеральный ядерный центр – ВНИИЭФ	2019	http://www.iprbookshop.ru/101929.html
6.1.2 Дополнительная учебная литература				
Фомин, Д. В.	Информационная безопасность	Саратов: Вузовское образование	2018	http://www.iprbookshop.ru/77320.html
Гультяева, Т. А.	Основы защиты информации	Новосибирск: Новосибирский государственный технический университет	2018	http://www.iprbookshop.ru/91638.html
Прохорова, О. В.	Информационная безопасность и защита информации	Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ	2014	http://www.iprbookshop.ru/43183.html
Аверченков, В. И., Рытов, М. Ю.	Организационная защита информации	Брянск: Брянский государственный технический университет	2012	http://www.iprbookshop.ru/7002.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
Компьютерный класс	Мультимедийное оборудование, компьютерная техника с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду
Лекционная аудитория	Мультимедийное оборудование, специализированная мебель, доска