

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.16	Информационная безопасность и защита компьютерной информации
----------------	--

Учебный план: _____ ФГОС3++b090302Г-12_26-14.plx

Кафедра: 32 Автоматизации технологических процессов и производств

Направление подготовки:
(специальность) 09.03.02 Информационные системы и технологии

Профиль подготовки:
(специализация) Геоинформационные системы и технологии

Уровень образования: бакалавриат

Форма обучения: очная

План учебного процесса

Семестр (курс для ЗАО)		Контактная работа обучающихся		Сам. работа	Контроль, час.	Трудоё мкость, ЗЕТ	Форма промежуточной аттестации
		Лекции	Практ. занятия				
6	УП	24	24	59,75	0,25	3	Зачет
	РПД	24	24	59,75	0,25	3	
Итого	УП	24	24	59,75	0,25	3	
	РПД	24	24	59,75	0,25	3	

Рабочая программа дисциплины составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 09.03.02 Информационные системы и технологии, утверждённым приказом Минобрнауки России от 19.09.2017 г. № 926

Составитель (и):

Кандидат технических наук,

Морева Светлана
Леонидовна

От кафедры составителя:

Заведующий кафедрой автоматизации
технологических процессов и производств

Ковалев Д.А.

От выпускающей кафедры:

Заведующий кафедрой

Ковалев Д.А.

Методический отдел:

Фахретдинова А. Р.

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 компьютерной информации.

1.2 Задачи дисциплины:

Рассмотреть существующие угрозы информационной безопасности информации в геоинформационных системах;

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

Приобрести практические навыки работы по защите информации в геоинформационных системах.

1.3 Требования к предварительной подготовке обучающегося:

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

2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ПК-3: Способен планировать изменения сетевых устройств информационно-коммуникационных систем предметными специалистами из других областей

Знать: терминологию в области информационной безопасности, методы и средства обеспечения информационной безопасности, методы нарушения конфиденциальности, целостности и доступности информации. Содержание основных понятий по правовому обеспечению информационной безопасности; основы безопасности операционных систем; основы безопасности вычислительных сетей; основные технические средства и методы защиты информации; основные программно-аппаратные средства обеспечения информационной безопасности

Уметь: правильно проводить анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, применять на практике основные общеметодологические принципы теории информационной безопасности.

Владеть: навыками по выполнению полного объема работ, связанного с комплексным обеспечением информационной безопасности ИС на основе разработанных программ и методик, в том числе с обеспечением требований нормативных документов, регламентирующих режим соблюдения государственной тайны

3 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование и содержание разделов, тем и учебных занятий	Семестр (курс для ЗАО)	Контактная работа		СР (часы)	Форма текущего контроля
		Лек. (часы)	Пр. (часы)		
Раздел 1. Основы информационной безопасности	6				Л
Тема 1. Теоретические основы информационной безопасности. Определения и составляющие информационной безопасности. Доступность, целостность, конфиденциальность.		3	3	8	
Тема 2. Актуальность защиты компьютерной информации. Важность и сложность проблемы информационной безопасности. Анализ проблематики, связанной с информационной безопасностью.		3	4	6	
Раздел 2. Угрозы информационной безопасности					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».		3	2	8,75	
Тема 4. Вредоносное программное обеспечение. Основные правила защиты от «компьютерных вирусов». Обзор и методика использования антивирусных программ.		3	3	9	
Раздел 3. Законодательство в области информационной безопасности					О,Л
Тема 5. Обзор российского законодательства в области цифровой и интеллектуальной ИБ. Ответственность на нарушения ИБ.		3	3	5	
Тема 6. Лицензирование и сертификация в информационной безопасности.		3	3	5	
Раздел 4. Программно-технические меры обеспечения компьютерной безопасности					Л
Тема 7. Технические средства защиты компьютерной информации.		3	3	9	

Тема 8. Программно-технические меры защиты информации		3	3	9	
Итого в семестре (на курсе для ЗАО)		24	24	59,75	
Консультации и промежуточная аттестация (Зачет)		0,25			
Всего контактная работа и СР по дисциплине		48,25		59,75	

4 КУРСОВОЕ ПРОЕКТИРОВАНИЕ

Курсовое проектирование учебным планом не предусмотрено

5 БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА ОЦЕНИВАНИЯ

6. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ, КРИТЕРИЕВ, СИСТЕМЫ И СРЕДСТВ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ

6.1 Показатели оценивания

Код компетенции	Показатели оценивания результатов обучения
ПК-3	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 геоинформационных системах. 3. Использует теоретические знания по обеспечению безопасности информации в геоинформационных системах для решения практических задач.

6.2 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 компьютерной 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 не способен 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.

6.3 Типовые контрольные задания и/или иные материалы, используемые для оценки результатов обучения

6.3.1 Типовые контрольные вопросы

№ п/п	Формулировки вопросов
Семестр 6	
1	Сформулируйте понятия и основные составляющие информационной безопасности
2	Определите понятия «безопасность информации» и его отличие от понятия «защита информации»
3	Сформулируйте текущее состояние российского законодательства в области информационной безопасности систем управления
4	Сформулируйте понятия «доступность», «целостность», «конфиденциальность информации»
5	Обоснуйте важность проблемы компьютерной информационной безопасности

6	В каком случае сотрудник учреждения может быть привлечен к ответственности за нарушения правил информационной безопасности?
7	Назовите наиболее распространенные угрозы для компьютерной информации
8	Назовите наиболее распространенные пути и каналы утечки компьютерной информации геоинформационных систем
9	Назовите виды атак и методы взлома информационных сетей злоумышленниками
10	Сформулируйте понятие законодательного уровня информационной безопасности
11	Какие Вы знаете категории и носители информации
12	Сформулируйте виды противников или «нарушителей» информационной безопасности
13	Назовите современные антивирусные программы
14	Сформулируйте достоинства и недостатки современных антивирусных программ
15	Назовите требования российского законодательства в области лицензирования и сертификации

6.3.2 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.

6.3.3 Типовые практико-ориентированные задания (задачи, кейсы)

Не предусмотрено

6.4 Методические материалы, определяющие процедуры оценивания результатов обучения

6.4.1 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»

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

6.4.2 Форма проведения промежуточной аттестации по дисциплине

Устная ☐ + Письменная ☐ + Компьютерное тестирование ☐ Иная ☐

6.4.3 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.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
7.1.1 Основная учебная литература				

Жук А.П., Жук Е.П., Лепешкин О.М. и др.	Защита информации	Москва: ИЦ РИО	2021	https://ibooks.ru/reading.php?short=1&productid=361250
Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование	2019	https://www.iprbookshop.ru/87995.html
7.1.2 Дополнительная учебная литература				
Морева С. Л.	Защита информации.	Санкт-Петербург: СПбГУПТД	2020	http://publish.sutd.ru/tp_ext_inf_publish.php?id=20205125
С.Л. Морева	Защита информации : практикум	М-во науки и высшего образования РФ, С.-Петербург. гос. ун-т пром. технологий и дизайна, Высш. шк. технологии и энергетики. - Санкт-Петербург : ВШТЭ СПбГУПТД	2020	http://nizrp.narod.ru/metod/kafinfizmtex/1632862450.pdf
Акимова, О. Ю.	Хранение и защита компьютерной информации	Москва: Издательский Дом МИСиС	2020	http://www.iprbookshop.ru/106895.html

7.2 Перечень профессиональных баз данных и информационно-справочных систем

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

7.3 Перечень лицензионного и свободно распространяемого программного обеспечения

MicrosoftWindows 8
 MicrosoftOfficeProfessional 2013

7.4 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