

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.О.24 Информационная безопасность

Учебный план: _____ ФГОС3++b090303-1_23-14.plx

Кафедра: Информационно-измерительных технологий и систем управления

Направление подготовки:
(специальность) 09.03.03 Прикладная информатика

Профиль подготовки:
(специализация) Искусственный интеллект в информационных системах

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					
8	УП	18	36	18	36	3	Экзамен
	РПД	18	36	18	36	3	
Итого	УП	18	36	18	36	3	
	РПД	18	36	18	36	3	

Рабочая программа дисциплины составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 09.03.03 Прикладная информатика, утверждённым приказом Минобрнауки России от 19.09.2017 г. № 922

Составитель (и):

Кандидат технических наук, доцент

Морева С.Л.

От кафедры составителя:

Заведующий кафедрой информационно-измерительных технологий и систем управления

Сидельников В.И.

От выпускающей кафедры:

Заведующий кафедрой

Сидельников В.И.

Методический отдел:

Смирнова В.Г.

1 ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1 Цель дисциплины: Целью дисциплины является изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах; ознакомление студентов с моделями возможных угроз, терминологией и основными понятиями теории безопасности информации, а так же с нормативными документами России по данному вопросу.

1.2 Задачи дисциплины:

Получение студентами знаний по существующим угрозам безопасности информации, подбору и применению современных методов и способов защиты информации; формирование практических умений и навыков применения современных технологий обеспечения защиты информации в системах управления.

1.3 Требования к предварительной подготовке обучающегося:

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

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

Информационные системы и технологии

Проектирование информационных систем

Измерительно-информационные средства для систем управления

Программные средства обработки информации

2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;
Знать: основные виды и классификацию угроз информационной безопасности
Уметь: использовать безопасные методы работы в Интернете и с электронными почтовыми сервисами
Владеть: навыками использования методов защиты информации различными способами
ОПК-4: Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью;
Знать: классификацию угроз в зависимости от обрабатываемой информации, способа ее хранения и средств обработки
Уметь: использовать нормативные документы в области защиты информации и в информационной безопасности
Владеть: навыками применения методов аудита организации защиты информации на предприятии

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	8					О
Тема 1. Теоретические основы информационной безопасности. Современное состояние защиты информации. Понятие, основные определения и составляющие информационной безопасности. Доступность, целостность, конфиденциальность.		1	3	1,5		
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	3	1,5	ГД	
Раздел 2. Угрозы информационной безопасности						
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	2	ГД	
Тема 4. Вредоносное программное обеспечение. Основные правила защиты от «компьютерных вирусов». Обзор и методика использования антивирусных программ. Восстановление пораженных «компьютерными вирусами» объектов.	2	4	2			
Раздел 3. Законодательство в области информационной безопасности					О	

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.		3	4	2		
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	3		
Раздел 4. Программно-технические меры обеспечения компьютерной безопасности						
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	3		
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	3		О,Т
Итого в семестре (на курсе для ЗАО)		18	36	18		
Консультации и промежуточная аттестация (Экзамен)		2,5		33,5		
Всего контактная работа и СР по дисциплине		56,5		51,5		

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
ОПК-3	Имеет представление об основных видах угроз информационной безопасности. Формулирует безопасные методы работы в Интернете и с электронными почтовыми сервисами. Демонстрирует навыки использования методов шифрования и дешифрования информации различными способами.	Вопросы устного собеседования. Тестовые задания.
ОПК-4	Знает классификацию угроз в зависимости от обрабатываемой информации, способа ее хранения и средств обработки. Объясняет применение нормативных документов в области защиты информации и информационной безопасности. Владеет навыками применения методов аудита организации защиты информации на предприятии.	Вопросы устного собеседования. Тестовые задания.

5.1.2 Система и критерии оценивания

Шкала оценивания	Критерии оценивания сформированности компетенций	
	Устное собеседование	Письменная работа
5 (отлично)	Обучающийся свободно ориентируется в основных понятиях и терминах по защите информационной безопасности; знает распространенные угрозы и пути и утечки информации; угрозы в зависимости от обрабатываемой информации, способа ее хранения и средств обработки; знает и применяет методы работы в Интернете и с электронными почтовыми сервисами; усвоил и применяет нормативные документы в области защиты информации; знаком с различными методами шифрования и дешифрования информации; владеет методами аудита организации защиты информации на предприятии.	Обучающийся полностью выполнил тестовое задание.
4 (хорошо)	Обучающийся хорошо ориентируется в основных понятиях и терминах по защите информационной безопасности; знает основные угрозы и пути и утечки информации; угрозы в зависимости от обрабатываемой информации, способа ее хранения и средств обработки; знает основные методы работы в Интернете и с электронными почтовыми сервисами; усвоил основную и знаком с дополнительной литературой по обеспечению информационной безопасности. Не знает методов аудита организации защиты информации на предприятии, возможно допустил несущественные ошибки в ответе на вопросы преподавателя.	Обучающийся выполнил тестовое задание, допустил несущественные ошибки.
3 (удовлетворительно)	Обучающийся плохо ориентируется в основных понятиях и терминах по защите информационной безопасности; слабо знает основные угрозы в зависимости от обрабатываемой информации, способа ее хранения и средств обработки; слабо усвоил основную литературу по обеспечению информационной безопасности. Не знает методы работы в Интернете и с электронными почтовыми сервисами; методы аудита организации защиты	Обучающийся выполнил тестовое задание, допустил существенные ошибки.

	информации на предприятии, допустил ошибки в ответе на вопросы преподавателя.	
2 (неудовлетворительно)	Обучающийся не знает основных понятий и терминов по защите информационной безопасности; слабо знает основные угрозы информации; не знает основную литературу по обеспечению информационной безопасности; не знает методы работы в Интернете и с электронными почтовыми сервисами; методы аудита организации защиты информации на предприятии, допустил серьезные ошибки в ответе на вопросы преподавателя.	Обучающийся не выполнил тестовое задание.

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 8	
1	Что такое информационная безопасность?
2	Какие предпосылки и цели обеспечения информационной безопасности?
3	В чем заключаются национальные интересы РФ в информационной сфере?
4	Какие пути решения проблем информационной безопасности РФ существуют?
5	Каковы общие принципы обеспечения защиты информации?
6	Какие имеются виды угроз информационной безопасности предприятия (организации)?
7	Какие существуют источники наиболее распространенных угроз информационной безопасности?
8	Что включают в себя требования по обеспечению комплексной системы информационной безопасности?
9	Какие уровни информационной защиты существуют, их основные составляющие?
10	В чем заключаются задачи криптографии?
11	Какие системы шифрования вы знаете?
12	Что включает в себя защита информации от несанкционированного доступа?
13	В чем заключаются достоинства и недостатки программно-аппаратных средств защиты информации?
14	Какие виды механизмов защиты могут быть реализованы для обеспечения идентификации и аутентификации пользователей?
15	Какие задачи выполняет подсистема управления доступом?
16	Какие требования предъявляются к подсистеме протоколирования аудита?
17	Какие виды механизмов защиты могут быть реализованы для обеспечения конфиденциальности данных и сообщений?
18	Какие функции выполняет служба регистрации и наблюдения?
19	Что такое информационно-опасные сигналы, их основные параметры?
20	Какие требования предъявляются к межсетевым экранам?
21	Какие имеются показатели защищенности межсетевых экранов?
22	Какая программа называется вирусом?
23	Какая атака называется атакой отказа в обслуживании?
24	Какие виды вирусов вы знаете?
25	Какие вирусы называются паразитическими?
26	Как распространяются вирусы?
27	Какие методы обнаружения вирусов вы знаете?
28	В чем заключается организация работ по защите от несанкционированного доступа интегрированной информационной системы управления предприятием?
29	Какие существуют пути защиты информации в локальной сети?
30	Из каких этапов состоят работы по обеспечению информационной безопасности предприятия?
31	Что понимают под политикой информационной безопасности?
32	Что включает в себя политика информационной безопасности РФ?
33	Какие нормативные документы РФ определяют концепцию защиты информации?

34	В каком случае сотрудник учреждения может быть привлечен к ответственности за нарушения правил информационной безопасности?
35	Сформулируйте понятия «доступность», «целостность», «конфиденциальность информации»
36	Назовите наиболее распространенные пути и каналы утечки информации систем управления.
37	Сформулируйте достоинства и недостатки современных антивирусных программ.
38	Назовите мероприятия по защите информации от несанкционированного доступа.
39	Назовите способы защиты информации от утечки по техническим каналам.
40	Объясните порядок оформления и получения сертификатов в области 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.

Коды, обладающие способностью к распространению (возможно, с изменениями) путем внедрения в другие программы, называются:

- а) вирусами
- б) руткитами
- в) червями

Уровень риска, который считается доступным для достижения желаемого результата, называется:

- а) устойчивостью
- б) терпимостью по отношению к риску
- в) независимостью

Код, способный самостоятельно, то есть без внедрения в другие программы, вызвать распространение своих копий по информационной системе и их выполнение, называется:

- а) Троянской программой
- б) червем
- в) вирусом

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»

Допуском обучающегося к промежуточной аттестации является сдача отчетов по практическим работам.

5.3.2 Форма проведения промежуточной аттестации по дисциплине

Устная + Письменная + Компьютерное тестирование Иная

5.3.3 Особенности проведения промежуточной аттестации по дисциплине

Время подготовки теста – 20 минут.

При проведении экзамена время, отводимое на подготовку к ответу, составляет не более 40 мин.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
6.1.1 Основная учебная литература				
Фомин, Д. В.	Информационная безопасность	Саратов, Москва: Профобразование, Ай Пи Ар Медиа	2022	https://www.iprbooks.hop.ru/118458.html
Суворова, Г. М.	Основы информационной безопасности	Саратов: Профобразование	2021	http://www.iprbooks.hop.ru/108005.html
Ревнивых, А. В.	Информационная безопасность в организациях	Москва: Ай Пи Ар Медиа	2021	http://www.iprbooks.hop.ru/108227.html
6.1.2 Дополнительная учебная литература				
Куликов, С. С.	Информационная безопасность локальных компьютерных сетей	Воронеж: Воронежский государственный технический университет, ЭБС АСВ	2021	https://www.iprbooks.hop.ru/118614.html
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

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