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

УТВЕРЖДАЮ
Первый проректор, проректор по УР
_____А.Е. Рудин
«30» 06 2020 года

Рабочая программа дисциплины

Б1.О.24 Информационная безопасность

Учебный план: ФГОС 3++2020-2021_09.03.03_ИИТА_ОЗО_ПИД.plx

Кафедра: 1 Автоматизации производственных процессов

Направление подготовки: (специальность) 09.03.03 Прикладная информатика

Профиль подготовки: (специализация) Прикладная информатика в дизайне

Уровень образования: бакалавриат

Форма обучения: очно-заочная

План учебного процесса

Семестр (курс для ЗАО)		Контактная работа обучающихся		Сам. работа	Контроль, час.	Трудоёмкость, ЗЕТ	Форма промежуточной аттестации
		Лекции	Практ. занятия				
10	УП	18	18	36	36	3	Экзамен
	РПД	18	18	36	36	3	
Итого	УП	18	18	36	36	3	
	РПД	18	18	36	36	3	

Санкт-Петербург
2020

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

Составитель (и):

доктор технических наук, Профессор	_____	Кикин Андрей Борисович
От кафедры составителя: Заведующий кафедрой автоматизации производственных процессов	_____	Энтин Виталий Яковлевич
От выпускающей кафедры: Заведующий кафедрой	_____	Сошников Антон Владимирович

Методический отдел:

_____

1 ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1 Цель дисциплины: Сформировать компетенции обучающегося в области основных общеметодологических основ информационной безопасности, а также базовых методов и средств защиты конфиденциальности, целостности и доступности информации.

1.2 Задачи дисциплины:

- Рассмотреть основные принципы и методы обеспечения информационной безопасности;
- Раскрыть принципы анализа угроз информационной безопасности;
- Рассмотреть методы защиты конфиденциальности, целостности и доступности информации;
- Показать особенности технологий и средств обеспечения информационной безопасности.

1.3 Требования к предварительной подготовке обучающегося:

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

Операционные системы, сети и телекоммуникации

Алгоритмизация и программирование

Информационные системы и технологии

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 шифрования и дешифрования 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. Основные понятия и методы защиты от угроз ИБ	10					О
Тема 1. Введение в информационную безопасность. Основные определения. Базовые свойства защищаемой информации. Методы защиты информации. Угрозы информационной безопасности. Классификация угроз.		2		3		
Тема 2. Система защиты от угрозы нарушения конфиденциальности. Организационные меры. Идентификация и аутентификация. Особенности парольных систем защиты. Стойкость парольных систем. Методы хранения и передачи паролей.		2		3		
Тема 3. Методы разграничения доступа. Методы обеспечения конфиденциальности. Симметричные и асимметричные криптосистемы. Системы распределения ключей. Построение системы защиты от угроз нарушения целостности, цифровые подписи.		2		3		

Тема 4. Методы защиты внешнего периметра. Системы обнаружения вторжений. Протоколирование и аудит. Построение системы защиты от угроз нарушения доступности. Методы создания избыточной информации. Дублирование и резервирование.		2		3		
Раздел 2. Основы криптографии и криптоанализа						
Тема 5. Криптология, криптография и криптоанализ – основные определения. История шифрования. Этапы: наивный, формальный, научный, компьютерный. Практические занятия: шифр Цезаря, квадрат Полибия, таблица Виженера.		2	4	4		
Тема 6. Современные алгоритмы симметричного шифрования. Блочные алгоритмы. Ячейка Фейстала. Алгоритм DES и ГОСТ 28147-89. Криптостойкость. Принципы хранения и передачи ключей симметричного шифрования. Практические занятия: шифрование методом гаммирования, сети Фейстала.		2	2	4	ИЛ	Т
Тема 7. Асимметричные криптосистемы. Алгоритм RSA. Комбинированные методы шифрования. Ключевые схемы. Технология ЭЦП. Криптографические хэш- функции.		2		4		
Тема 8. Проблема подмены открытого ключа ЭЦП. Сертификация, иерархия и инфраструктура открытых ключей. Комплексный метод защиты.		2		4		
Раздел 3. Правовые и нормативные основы ИБ						
Тема 9. Законодательство РФ и нормативные акты в сфере ИБ. Информация с ограниченным доступом (государственная тайна, служебная, коммерческая и т. д.). Персональные данные.		2		4		Т
Тема 10. Практические занятия: Основные типы файлов. Методы определения истинного типа файлов без учета расширений. Простейшие способы редактирования исполняемых файлов. Виды вредоносных программ. Антивирусная защита.			12	4	ИЛ	
Итого в семестре (на курсе для ЗАО)		18	18	36		
Консультации и промежуточная аттестация (Экзамен)		2,5		33,5		
Всего контактная работа и СР по дисциплине		38,5		69,5		

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	Оценивает и характеризует возможные угрозы информационной безопасности. Применяет комплекс мер для безопасной работы и защиты оборудования и данных от несанкционированного доступа. Обосновывает выбор конкретного криптографического средства.	Вопросы для устного собеседования. Практическое задание.
ОПК-4	Объясняет основные принципы определения актуальных угроз информационной безопасности. Проводит анализ потенциально-возможных угроз информации на основе нормативно-правовой базы. Выстраивает алгоритм проведения аудита информационной безопасности в организации.	Вопросы для устного собеседования. Практическое задание.

5.1.2 Система и критерии оценивания

Шкала оценивания	Критерии оценивания сформированности компетенций	
	Устное собеседование	Письменная работа
5 (отлично)	Полный, исчерпывающий ответ, явно демонстрирующий глубокое понимание предмета и широкую эрудицию в оцениваемой области. Критический, оригинальный подход к материалу.	
4 (хорошо)	Ответ полный, в целом качественный, основанный на проработке всех обязательных источников информации. Подход к материалу ответственный, но стандартный. Могут присутствовать небольшие пробелы в знаниях или несущественные ошибки.	
3 (удовлетворительно)	Ответ неполный, основанный только на лекционных материалах. Демонстрирует понимание сущности предмета в целом, без углубления в детали. Присутствуют существенные ошибки или пробелы в знаниях по некоторым темам, незнание важных терминов.	
2 (неудовлетворительно)	Непонимание заданного вопроса. Неспособность ответить на вопрос без помощи экзаменатора. Незнание значительной части принципиально важных элементов дисциплины. Многочисленные грубые ошибки. Неспособность сформулировать хотя бы отдельные концепции дисциплины. Попытка списывания, использования неразрешенных технических устройств или пользования подсказкой другого человека (вне зависимости от успешности такой попытки).	

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 10	
1	Введение в информационную безопасность. Основные определения. Базовые свойства защищаемой информации.
2	Методы защиты информации. Угрозы информационной безопасности. Классификация угроз.
3	Система защиты от угрозы нарушения конфиденциальности. Организационные меры.
4	Идентификация и аутентификация. Особенности парольных систем защиты.
5	Стойкость парольных систем. Методы хранения и передачи паролей.
6	Методы разграничения доступа. Криптографические методы обеспечения конфиденциальности.
7	Симметричные и асимметричные криптосистемы. Системы распределения ключей.
8	Построение системы защиты от угроз нарушения целостности: цифровые подписи, коды проверки подлинности.
9	Методы защиты внешнего периметра. Системы обнаружения вторжений. Протоколирование и аудит.

10	Построение системы защиты от угроз нарушения доступности. Методы создания избыточной информации.
11	Дублирование и резервирование информации.
12	Криптология, криптография и криптоанализ – основные определения.
13	История шифрования. Этапы: наивный, формальный, научный, компьютерный.
14	Современные алгоритмы симметричного шифрования. Блочные алгоритмы. Ячейка Фейстала.
15	Алгоритмы шифрования DES и ГОСТ 28147-89.
16	Криптостойкость. Принципы хранения и передачи ключей симметричного шифрования.
17	Асимметричные криптосистемы. Алгоритм RSA.
18	Комбинированные методы шифрования. Ключевые схемы. Комплексный метод защиты информации.
19	Проблема подмены открытого ключа ЭЦП. Сертификация, иерархия и инфраструктура открытых ключей.
20	Законодательство РФ и нормативные акты в сфере ИБ. Информация с ограниченным доступом. Персональные данные.
21	Технология ЭЦП. Криптографические хэш-функции.
22	Виды вредоносных программ. Антивирусная защита.

5.2.2 Типовые тестовые задания

1) Определить истинный тип файлов (из базы на сервере кафедры АПП)
Файл Тип файла Расширение
---
file008 | |
file020 | |
file028 | |
file030 | |
file051 | |
file058 | |
file062 | |
file064 | |
file084 | |
file085 | |

2) Определить истинный тип файлов (из базы на сервере кафедры АПП)

Файл	Тип файла	Расширение
file009		
file022		
file023		
file048		
file049		
file070		
file072		
file080		
file085		
file097		

3) Определить истинный тип файлов (из базы на сервере кафедры АПП)

Файл	Тип файла	Расширение
file006		
file013		
file016		
file023		
file045		
file078		
file082		
file085		
file096		
file099		

4) Определить истинный тип файлов (из базы на сервере кафедры АПП)

Файл	Тип файла	Расширение
file013		
file017		
file028		
file047		
file053		
file055		
file080		
file087		
file092		
file093		

5.2.3 Типовые практико-ориентированные задания (задачи, кейсы)

1. Расшифровать, используя таблицу Виженера следующую криптограмму:

а) Ключ: АМЕРИКА

Шифрограмма:
МЗФДЙЦИКАЙЭШЩДБЫХЫЬУЗВЗЦЫИТЫВМТЩТЬДЕШЕЮЦЁХВЮЖЯНМРЕЩДТЪЩВЕЭЭХЦШОССХМНТНОЦЩЯЩЧЕ

(Исходный текст: мы публикуем подборку из высказываний сделанных в свое время в совершенно серьезной форме)

б) Ключ: ЕВРОПА

Шифрограмма: ИВНБЮБАНЯАЪАМВЮЭСПУНЮУБЕХЮХЦЭОНРСЭБНУДРЬЭОИНПАСОЙЕЯРАЕСЖЮЧ

(Исходный текст: да это было сказано вполне серьезно и обоснованно для своего времени)

в) Ключ: АЗИЯ

Шифрограмма:ИХЫДРМЪМОЗАСОИЬГЕЪКЪЗГКЯТДЬМАЩЬКЫИУТИПЫНГЦАСОКЧБОШСССЖЪДГЦММЯ

(Исходный текст: интересно а что будет вызывать у нас улыбку из того что говорится сегодня)

2. Одним из реквизитов электронного документа является электронно-цифровая подпись (ЭЦП).
- Какова технология получения ЭЦП?
- Что такое сертификат ЭЦП?
- Что обеспечивается с помощью ЭЦП?

3. Основным методом защиты конфиденциальности информации является криптография.
- Перечислите основные методы криптографической защиты информации.
- Перечислите недостатки и преимущества симметричных и асимметричных криптосистем.
- В каком случае метод гаммирования дает абсолютную криптостойкость?

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

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
6.1.1 Основная учебная литература				
Прохорова, О. В.	Информационная безопасность и защита информации	Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ	2014	http://www.iprbookshop.ru/43183.html
Басалова Г. В.	Основы криптографии	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ)	2016	http://www.iprbookshop.ru/52158.html
Нестеров С.А.,	Основы информационной безопасности	Санкт-Петербург: Санкт-Петербургский политехнический университет Петра Великого	2014	http://www.iprbookshop.ru/43960.html
6.1.2 Дополнительная учебная литература				
Кикин А.Б.	Хранение и защита компьютерной информации	СПб.: СПбГУПТД	2015	http://publish.sutd.ru/tp_ext_inf_publish.php?id=2807
Кикин А. Б.	Информационная безопасность. Основы криптографии	СПб.: СПбГУПТД	2019	http://publish.sutd.ru/tp_ext_inf_publish.php?id=201932
Башлы, П. Н., Бабаш, А. В., Баранова, Е. К.	Информационная безопасность и защита информации	Москва: Евразийский открытый институт	2012	http://www.iprbookshop.ru/10677.html

6.2 Перечень профессиональных баз данных и информационно-справочных систем

1. Электронно-библиотечная система СПбГУПТД [Электронный ресурс]. URL: http://publish.sutd.ru/
2. Электронно-библиотечная система IPRbooks [Электронный ресурс]. URL: http://www.iprbookshop.ru/
3. Информационная система «Единое окно доступа к образовательным ресурсам. Раздел. Информатика и информационные технологии» [Электронный ресурс]. URL: http://window.edu.ru/catalog/?p_rubr=2.2.75.6
4. Официальный интернет-портал правовой информации (федеральная государственная информационная система) [Электронный ресурс]. URL: http://pravo.gov.ru

6.3 Перечень лицензионного и свободно распространяемого программного обеспечения

Microsoft Windows

Far

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