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

УТВЕРЖДАЮ
Первый проректор,
проректор по учебной работе

_____ А.Е. Рудин

«30» 06 2020

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.12	Хранение и защита компьютерной информации
(Индекс дисциплины)	(Наименование дисциплины)

Кафедра: 1 (Код) Автоматизации производственных процессов (Наименование кафедры)

Направление подготовки: 15.04.04 Автоматизация технологических процессов и производств

Профиль подготовки: Автоматизация и управление

Уровень образования: Магистратура

План учебного процесса

Составляющие учебного процесса		Очное обучение	Очно-заочное обучение	Заочное обучение
Контактная работа обучающихся с преподавателем по видам учебных занятий и самостоятельная работа обучающихся (часы)	Всего	**72**		
	Аудиторные занятия	**34**		
	Лекции			
	Лабораторные занятия	17		
	Практические занятия	17		
	Самостоятельная работа	**38**		
	Промежуточная аттестация			
Формы контроля по семестрам (номер семестра)	Экзамен			
	Зачет	1		
	Контрольная работа			
	Курсовой проект (работа)			
Общая трудоемкость дисциплины (зачетные единицы)		**2**		

Форма обучения:	Распределение зачетных единиц трудоемкости по семестрам											
	1	2	3	4	5	6	7	8	9	10	11	12
Очная	**2**											
Очно-заочная												
Заочная												

Санкт-Петербург
2020

Рабочая программа составлена в соответствии с федеральным государственным образовательным стандартом высшего образования
по направлению: 15.04.04 Автоматизация технологических процессов и производств

1. ВВЕДЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

1.1. Место преподаваемой дисциплины в структуре образовательной программы

Блок 1: Базовая [ ] Обязательная [X] Дополнительно является факультативом [ ]
Вариативная [X] По выбору [ ]

1.2. Цель дисциплины

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

1.3. 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.

1.4. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Код компетенции	Формулировка компетенции	Этап формирования
ПК-9	Способностью обеспечивать надежность и безопасность на всех этапах жизненного цикла продукции, выбирать системы экологической безопасности производства	1
Планируемые результаты обучения Знать: Базовые методы и средства хранения и защиты компьютерной информации. Уметь: Проводить организационные мероприятия по защите информации. Владеть: Навыками криптографических методов защиты информации.		

1.5. Дисциплины (практики) образовательной программы, в которых было начато формирование компетенций, указанных в п.1.4:

Информационные системы управления качеством в автоматизированных и автоматических производствах (ПК-9)
Распределенные компьютерные информационно-управляющие системы (ПК-9)

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение
Учебный модуль 1. Основные понятия и виды угроз ИБ.			
Тема 1. Введение в информационную безопасность. Основные определения. Базовые свойства защищаемой информации. Методы защиты информации. Угрозы информационной безопасности. Классификация угроз.	8		
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.	6		
Тема 3. Методы разграничения доступа. Криптографические методы обеспечения конфиденциальности. Симметричные и асмметричные криптосистемы. Си-	8		

Наименование и содержание учебных модулей, тем и форм контроля	Объем (часы)		
	очное обучение	очно-заочное обучение	заочное обучение
стемы распределения ключей. Построение системы защиты от угроз нарушения целостности: цифровые подписи, криптографические хэш-функции, коды проверки подлинности.			
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.	8		
Текущий контроль 1 (опрос)	1		
Учебный модуль 2. Автоматизация синтеза систем.			
Тема 5. Криптология, криптография и криптоанализ – основные определения. История шифрования. Этапы: наивный, формальный, научный, компьютерный.	8		
Тема 6. Современные алгоритмы симметричного шифрования. Блочные алгоритмы. Ячейка Фейстала. Алгоритм DES и ГОСТ 28147-89. Криптостойкость. Принципы хранения и передачи ключей симметричного шифрования.	10		
Тема 7. Асимметричные криптосистемы. Алгоритм RSA. Комбинированные методы шифрования. Ключевые схемы.	8		
Тема 8. Проблема подмены открытого ключа ЭЦП. Сертификация, иерархия и инфраструктура открытых ключей. Комплексный метод защиты.	8		
Текущий контроль 2 (тестирование)	1		
Промежуточная аттестация по дисциплине (зачет)	6		
ВСЕГО:	**72**		

3. ТЕМАТИЧЕСКИЙ ПЛАН

3.1. Лекции

Не предусмотрены

3.2. Практические занятия

Номера изучаемых тем	Наименование и форма занятий	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
1	Исследование особенностей парольных систем аутентификации.	1	4				
4	Восстановление зашифрованных файлов.	1	5				
6	Блочные методы шифрования – сети Фейстала.	1	4				
7	Изучение криптографическая хэш-функция MD-5	1	4				
	ВСЕГО:		**17**				

3.3. Лабораторные занятия

Номера изучаемых тем	Наименование лабораторных занятий	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
2	Изучение методов определения истинного типа различных файлов без учета расширений.	1	4				
3	Использование HEX редакторов в простейших случаях для редактирования исполняемых файлов.	1	4				
5	Практикум по шифрованию: квадрат Полибия, таблица	1	5				

Номера изучаемых тем	Наименование лабораторных занятий	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
	Виженера.						
5	Потоковое шифрование методом гаммирования, использование XOR	1	4				
	ВСЕГО:		**17**				

4. КУРСОВОЕ ПРОЕКТИРОВАНИЕ

Не предусмотрено

5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ ОБУЧАЮЩЕГОСЯ

номера учебных модулей, по которым проводится контроль	Форма контроля знаний	Очное обучение		Очно-заочное обучение		Заочное обучение	
		Номер семестра	Кол-во	Номер семестра	Кол-во	Номер семестра	Кол-во
1	Опрос	1	1				
2	Тестирование	1	1				

6. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ

Виды самостоятельной работы обучающегося	Очное обучение		Очно-заочное обучение		Заочное обучение	
	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)	Номер семестра	Объем (часы)
Усвоение теоретического материала	1	16				
Подготовка к практическим и лабораторным занятиям	1	16				
Подготовка к зачету	1	6				
ВСЕГО:		**38**				

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

7.1. Характеристика видов и используемых инновационных форм учебных занятий

Наименование видов учебных занятий	Используемые инновационные формы	Объем занятий в инновационных формах (часы)		
		очное обучение	очно-заочное обучение	заочное обучение
Лекции	Не предусмотрены			
Практические и семинарские занятия	Обсуждение тем, приведенных в табл.3.2. Поиск вариантов решения проблемных ситуаций.	4		
Лабораторные занятия	Индивидуальная работа с компьютерными программами в интерактивном режиме под руководством преподавателя.	4		
	ВСЕГО:	8		

7.2. Балльно-рейтинговая система оценивания успеваемости и достижений обучающихся

№ п/п	Вид деятельности обучающегося	Весовой коэффициент значимости, %	Критерии (условия) начисления баллов
1	Аудиторная активность: посещение лабораторных и практических занятий, прохождение текущего контроля	30	• 4 балла за каждое занятие (всего 17 занятий), максимум 68 баллов • 2 балла за каждый правильный ответ на вопрос текущего контроля (всего 16 вопросов), максимум 32 баллов
2	Подготовка и представление устных докладов, либо участие в студенческой конференции «Дни науки» с публикацией тезисов доклада	20	• 50 баллов за доклад на занятии (всего 1 доклад в семестре), максимум 50 баллов; • 30 баллов за выступление на конференции, либо до 50 баллов за доклад, занявший одно из первых трех мест на конференции, максимум 50 баллов.
4	Сдача зачета	50	Ответ на вопросы зачета (полнота, владение терминологией, затраченное время) – максимум 100 баллов.
	Итого (%):	100	

Перевод балльной шкалы в традиционную систему оценивания

Баллы	Оценка по нормативной шкале	
86 - 100	5 (отлично)	Зачтено
75 – 85	4 (хорошо)	
61 – 74		
51 - 60	3 (удовлетворительно)	
40 – 50		
17 – 39	2 (неудовлетворительно)	Не зачтено
1 – 16		
0		

8. ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Учебная литература

а) основная учебная литература

3. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ Е.Б. Белов [и др.].— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2011.— 558 с. http://www.iprbookshop.ru/12014.— ЭБС «IPRbooks».

б) дополнительная учебная литература

Кикин А.Б. Хранение и защита компьютерной информации. [электронный ресурс] Методические указания к лабораторным работам / СПГУТД, СПб., 2015, 34 с. Режим доступа: http://publish.sutd.ru/tp_ext_inf_publish.php?id=2807, по паролю

Кикин А.Б. Информационная безопасность. [электронный ресурс] : СПГУТД, СПб., 2015 /Методические указания к лабораторным работам /, 32 с Режим доступа: http://publish.sutd.ru/tp_ext_inf_publish.php?id=2809, по паролю.

Кикин А.Б. Информационная безопасность.– Прикладная информатика (все профили) заочная форма обучения. СПГУТД, 2014,/ Методические указания для студентов направления/ 22 с. Режим доступа: http://publish.sutd.ru/tp_ext_inf_publish.php?id=1695

Кукина Е.Г. Введение в криптографию [Электронный ресурс]: Кукина Е.Г., Романьков В.А.— Электрон. текстовые данные.— Омск: Омский государственный университет, 2013 ,/сборник задач и упражнений/.— 91 с. Режим доступа: http://www.iprbookshop.ru/24876.— ЭБС «IPRbooks».

8.2. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

1 Программное обеспечение компьютерного класса кафедры АПП, разработанное НПР кафедры.

8.3. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины

1 http://publish.sutd.ru/

8.4. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Windows 10, OfficeStd

Far, Far Group

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

Лаборатория программирования. Компьютерный класс, видеопроекционная техника.

8.6. Иные сведения и (или) материалы

Не предусмотрены

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Виды учебных занятий и самостоятельная работа обучающихся	Организация деятельности обучающегося
Лекции	Не предусмотрены
Практические занятия	На практических занятиях обсуждаются темы, приведенные в табл.3.2. Осуществляется поиск вариантов решения проблемных ситуаций.
Лабораторные занятия	Лабораторные занятия способствуют развитию практических навыков владения изучаемыми методами. В процессе построения математической модели системы автоматического регулирования и численного моделирования ее динамики. На лабораторных работах обучающийся изучает процесс или объект на основе взаимодействия с его физической и математической моделью В результате проведения лабораторного занятия обучающийся должен понять возможности совершенствования системы управления объектом.
Самостоятельная работа	Данный вид работы предполагает расширение и закрепление знаний, умений и навыков, усвоенных на аудиторных занятиях путем самостоятельной проработки учебно-методических материалов по дисциплине и другим источникам информации, а также подготовки к зачету. Самостоятельная работа выполняется индивидуально, а также может проводиться под руководством преподавателя. При подготовке к зачету необходимо ознакомиться с перечнем вопросов, проработать рекомендуемую литературу, получить консультацию у преподавателя.

10. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

10.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

10.1.1. Показатели оценивания компетенций на этапах их формирования

Код компетенции / этап освоения	Показатели оценивания компетенций	Наименование оценочного средства	Представление оценочного средства в фонде
ПК-9 / первый этап	Формулирует основные принципы безопасного хранения информации. Составляет план защиты информации в конкретной ситуации. Применяет базовые способы шифрования/дешифрования информации.	Вопросы для устного собеседования Тестовые задания Тестовые задания.	Вопросы для собеседования (12). Тестовые-задания (3). Тестовые-задания (3).

10.1.2. Описание шкал и критериев оценивания сформированности компетенций

Критерии оценивания сформированности компетенций

40 – 100	Зачтено	Обучающийся своевременно выполнил лабораторные работы и представил результаты; в соответствии с требованиями.
0 – 39	Не зачтено	Обучающийся не выполнил (выполнил частично) лабораторные работы, допустил существенные ошибки в ответе на вопросы преподавателя.

10.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций

10.2.1. Перечень вопросов (тестовых заданий), разработанный в соответствии с установленными этапами формирования компетенций

№ п/п	Формулировка вопросов	№ темы
1	Введение в информационную безопасность. Основные определения. Базовые свойства защищаемой информации.	1
2	Методы защиты информации. Угрозы информационной безопасности. Классификация угроз.	1
3	Система защиты от угрозы нарушения конфиденциальности. Организационные меры. Идентификация и аутентификация. Особенности парольных систем защиты.	2
4	Стойкость парольных систем. Методы хранения и передачи паролей.	2
5	Методы разграничения доступа. Криптографические методы обеспечения конфиденциальности.	3
6	Симметричные и асмметричные криптосистемы. Системы распределения ключей.	3
7	Построение системы защиты от угроз нарушения целостности: цифровые подписи, криптографические хэш-функции, коды проверки подлинности.	4
8	Методы защиты внешнего периметра. Системы обнаружения вторжений. Протоколирование и аудит..	4
9	Построение системы защиты от угроз нарушения доступности. Методы создания избыточной информации. Дублирование и резервирование информации	5
10	Криптология, криптография и криптоанализ – основные определения. История шифрования. Этапы: наивный, формальный, научный, компьютерный	5
11	Современные алгоритмы симметричного шифрования. Блочные алгоритмы. Ячейка Фейстала..	6
12	Алгоритм шифрования DES и ГОСТ 28147-89.	6
13	Криптостойкость. Принципы хранения и передачи ключей симметричного шифрования	7
14	Асимметричные криптосистемы. Алгоритм RSA.	7
15	Комбинированные методы шифрования. Ключевые схемы. Комплексный метод защиты информации	8
16	Проблема подмены открытого ключа ЭЦП. Сертификация, иерархия и инфраструктура открытых ключей.	8

Вариант тестовых заданий, разработанных в соответствии с установленными этапами формирования компетенций

№ п/п	Формулировки теста	№ темы
	Определить истинный тип файлов (из базы на сервере кафедры АПП)	**1-5**

Файл	Тип файла	Расширение
file008		
file020		
file028		
file030		
file051		
file058		
file062		
file064		

	file084				
	file085				
	Определить истинный тип файлов (из базы на сервере кафедры АПП)				**1-5**
	file009				
	file022				
	file023				
	file048				
	file049				
	file070				
	file072				
	file080				
	file085				
	file097				
	Определить истинный тип файлов (из базы на сервере кафедры АПП)				**1-5**
	file006				
	file013				
	file016				
	file023				
	file045				
	file078				
	file082				
	file085				
	file096				
	file099				
	Определить истинный тип файлов (из базы на сервере кафедры АПП)				**1-5**
	file013				
	file017				
	file028				
	file047				
	file053				
	file055				
	file080				
	file087				
	file092				
	file093				

10.2.2. Перечень тем докладов *(рефератов, эссе, пр.)***, разработанных в соответствии с установленными этапами формирования компетенций**

Доклады не предусмотрены

Вариант типовых заданий (задач, кейсов), разработанных в соответствии с установленными этапами формирования компетенций

№ п/п	Условия типовых задач (кейсов)	Ответ
1	Расшифровать, используя таблицу Виженера следующие криптограммы:	

1.1	**Ключ:** АМЕРИКА **Шифрограмма:** МЗФДЙЦИКАЙЭШЩ ДБЫХЫЬУЗВЗЦЫИТЫВМТЩТЬД ЕШЕЮЦЁХВЮЖЯНМРЕЩДТЪЩВЕЭ ЭХЦШОССХМНТНОЦЩЯЩЧЕ	**Исходный текст:** мы публикуем подборку из высказываний сделанных в свое время в совершенно серьезной форме
1.2	**Ключ:** ЕВРОПА **Шифрограмма:** ИВНБЮБАНЯАЪАМ ВЮЭСПУНЮУБЕХЮХЦЭОНРСЭБ НУДРЬЭОИНПАСОЙЕЯРАЕСЖЮЧ	**Исходный текст:** да это было сказано вполне серьезно и обоснованно для своего времени
1.3	**Ключ:** АЗИЯ **Шифрограмма:**ИХЫДРМЪМОЗАСОИ ЬГЕЪКЪЗГКЯТДЬМАЩЬКЫИУТИ ПЫНГЦАСОКЧБОШСССЖЪДГЦММЯ	**Исходный текст:** интересно а что будет вызывать у нас улыбку из того что говорится сегодня
1.4	**Ключ:** АФРИКА **Шифрограмма:** ТФЫЧПУСЖБЧФСТЦЯ УККТЩЬНЯОНЭЭНПТСАЩБХОМБЮ ЧНОНЩФЧЬТАЖЫЧМЧТГСДЫАСЁЭИ ЭРИЦРЫЖЕГГЫИХСРЩФЪЭВОЁТЗТИ	
1.5	**Ключ:** АВСТРАЛИЯ **Шифрограмма:**ПРОЕЯМЯЪЦИФСРЗТЪ МЯНПАЧЩЗЪЙПЕФЦАЩЕЩНЗМЖЦЕЮ ИЦИЙОЛЗЧЮНЪЪСИ	
2	Одним из реквизитов электронного документа является электронно-цифровая подпись (ЭЦП).	
2.1	Какова технология получения ЭЦП?	
2.2	Что такое сертификат ЭЦП?	
2.3	Что обеспечивается с помощью ЭЦП?	
3	Основным методом защиты конфиденциальности информации является криптография.	
3.1	Перечислите основные методы криптографической защиты информации.	
3.2	Перечислите недостатки и преимущества симметричных и асимметричных криптосистем	
3.3	В каком случае метод гаммирования дает абсолютную криптостойкость?	

10.3. Методические материалы,
определяющие процедуры оценивания знаний, умений, владений (навыков и (или) практического опыта деятельности), характеризующих этапы формирования компетенций

10.3.1. Условия допуска обучающегося к сдаче зачета, защите курсового проекта и ликвидации академической задолженности

Положение о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся (принято на заседании Ученого совета 31.08.2013г., протокол № 1)

10.3.2. Форма проведения промежуточной аттестации по дисциплине

устная [X] письменная [ ] компьютерное тестирование [ ] иная* [ ]

**В случае указания формы «Иная» требуется дать подробное пояснение*

10.3.3. Особенности проведения зачета

- Допускается использование справочных материалов.
- Время на подготовку ответа на зачете не превышает 20 минут.