

УТВЕРЖДАЮ  
Первый проректор, проректор по  
УР

\_\_\_\_\_ А.Е. Рудин

«28» 06 2022 года

## Рабочая программа дисциплины

**Б1.В.ДВ.01.01** Информационная безопасность

Учебный план: 2022-2023 15.03.04 ИИТА АТПиУвМПК ОО №1-1-149.plx

Кафедра: **1** Автоматизации производственных процессов

Направление подготовки: 15.03.04 Автоматизация технологических процессов и производств  
(специальность)

Профиль подготовки: Автоматизация технологических процессов и управления в  
(специализация) многоотраслевых производственных комплексах

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	17	17	37,75	0,25	2	Зачет
	РПД	17	17	37,75	0,25	2	
Итого	УП	17	17	37,75	0,25	2	
	РПД	17	17	37,75	0,25	2	

Рабочая программа дисциплины составлена в соответствии с федеральным государственным образовательным стандартом высшего образования по направлению подготовки 15.03.04 Автоматизация технологических процессов и производств, утверждённым приказом Министерства образования и науки Российской Федерации от 09.08.2021 г. № 720

Составитель (и):

доктор технических наук, Профессор

\_\_\_\_\_

Кикин Андрей Борисович

От кафедры составителя:

Заведующий кафедрой  
производственных процессов

автоматизации

\_\_\_\_\_

Энтин Виталий  
Яковлевич

От выпускающей кафедры:

Заведующий кафедрой

\_\_\_\_\_

Энтин Виталий  
Яковлевич

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:

- Информационные технологии
- Программирование и алгоритмизация

## 2 КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

<b>ПК-1: Способен выполнить техническое задание на разработку автоматизированной системы управления технологическими процессами</b>
<b>Знать:</b> основные виды и классификацию угроз информационной безопасности при разработке автоматизированной системы управления технологическими процессами.
<b>Уметь:</b> использовать безопасные методы работы в Интернете и с электронной почтой при разработке автоматизированной системы управления технологическими процессами.
<b>Владеть:</b> навыками работы с методами зашифровывания и расшифровывания информации различными способами при разработке автоматизированной системы управления технологическими процессами.

## 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 виды угроз ИБ	6					О
Тема 1. Введение в информационную безопасность. Основные определения. Базовые свойства защищаемой информации. Методы защиты информации. Угрозы информационной безопасности. Классификация угроз.		2	2	4		
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	2	6	ИЛ	
Тема 3. Методы разграничения доступа. Криптографические методы обеспечения конфиденциальности. Симметричные и асимметричные криптосистемы. Системы распределения ключей. Построение системы защиты от угроз нарушения целостности: цифровые подписи, криптографические хэш-функции, коды проверки подлинности.		2	2	6		

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	2	4		
Раздел 2. Криптография и криптоанализ						
Тема 5. Криптология, криптография и криптоанализ – основные определения. История шифрования. Этапы: наивный, формальный, научный, компьютерный.		3	3	3,75	ИЛ	
Тема 6. Современные алгоритмы симметричного шифрования. Блочные алгоритмы. Ячейка Фейстала. Алгоритм DES и ГОСТ 28147-89. Криптостойкость. Принципы хранения и передачи ключей симметричного шифрования.		2	2	6		Т
Тема 7. Асимметричные криптосистемы. Алгоритм RSA. Комбинированные методы шифрования. Ключевые схемы. Технология ЭЦП.		2	2	4		
Тема 8. Проблема подмены открытого ключа ЭЦП. Сертификация, иерархия и инфраструктура открытых ключей. Комплексный метод защиты.		2	2	4		
Итого в семестре (на курсе для ЗАО)		17	17	37,75		
Консультации и промежуточная аттестация (Зачет)		0,25				
<b>Всего контактная работа и СР по дисциплине</b>		34,25		37,75		

#### 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-1	Повествует о решениях стандартных задач профессиональной деятельности по разработке автоматизированной системы управления технологическими процессами с учетом основных требований информационной безопасности. Определяет, какие факторы могут являться угрозой информационной безопасности автоматизированных систем. Выбирает безопасные методы просмотра сайтов, понимает опасности, связанные с вложениями электронной почты. Обосновывает выбор конкретного криптографического средства.	Вопросы для устного собеседования. Кейс-задания.

##### 5.1.2 Система и критерии оценивания

Шкала оценивания	Критерии оценивания сформированности компетенций	
	Устное собеседование	Письменная работа
Зачтено	Полный, исчерпывающий ответ, явно демонстрирующий глубокое понимание предмета и широкую эрудицию в оцениваемой области. Критический, оригинальный подход к материалу. Качество исполнения всех элементов задания полностью соответствует всем требованиям.	

Не зачтено	Неспособность ответить на вопрос без помощи экзаменатора. Незнание значительной части принципиально важных элементов дисциплины. Многочисленные грубые ошибки.	
------------	--	--

## 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 6	
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. Дублирование и резервирование информации.
11	Криптология, криптография и криптоанализ – основные определения. История шифрования. Этапы: наивный, формальный, научный, компьютерный.
12	Современные алгоритмы симметричного шифрования. Блочные алгоритмы. Ячейка Фейстала.
13	Алгоритмы шифрования DES и ГОСТ 28147-89.
14	Криптостойкость. Принципы хранения и передачи ключей симметричного шифрования.
15	Асимметричные криптосистемы. Алгоритм RSA.
16	Комбинированные методы шифрования. Ключевые схемы. Комплексный метод защиты информации.
17	Технология ЭЦП. Криптографические хэш-функции.
18	Проблема подмены открытого ключа ЭЦП. Сертификация, иерархия и инфраструктура открытых ключей.
19	Законодательство РФ и нормативные акты в сфере ИБ. Информация с ограниченным доступом. Персональные данные.
20	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
------	-----------	------------

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
------	-----------	------------

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
------	-----------	------------

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
------	-----------	------------

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:

МЗФДЙЦИКАЙЭШЩДБЫХЫЪУЗВЗЦЫИТЫВМТЩТЬДЕШЕЮЦЁХВЮЖЯНМРЕЩДТЬЦВЕЭЭХЦШОССХМНТНОЦ  
ЩЯЦЦЧЕ

(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:ИХЫДРМЪМОЗАСОИЪГЕЪКЪЗГКЯТДЪМАЦЬКЫИУТИПЫНГЦАСОКЧБОШСССЖЪДГЦМ

МЯ

(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

Для получения зачёта по дисциплине необходимо успешно выполнить два тестовых задания:

1) по определению истинного типа 10 файлов;

2) по расшифровке криптограммы с помощью таблицы Виженера.

## 6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### 6.1 Учебная литература

Автор	Заглавие	Издательство	Год издания	Ссылка
<b>6.1.1 Основная учебная литература</b>				
Шаньгин, В. Ф.	Информационная безопасность и защита информации	Саратов: Профобразование	2019	<a href="http://www.iprbookshop.ru/87995.html">http://www.iprbookshop.ru/87995.html</a>
Прохорова, О. В.	Информационная безопасность и защита информации	Самара: Самарский государственный архитектурно-строительный университет, ЭБС АСВ	2014	<a href="http://www.iprbookshop.ru/43183.html">http://www.iprbookshop.ru/43183.html</a>
Артемов, А. В.	Информационная безопасность	Орел: Межрегиональная Академия безопасности и выживания (МАБИВ)	2014	<a href="http://www.iprbookshop.ru/33430.html">http://www.iprbookshop.ru/33430.html</a>
Горюхина, Е. Ю., Литвинова, Л. И., Ткачева, Н. В.	Информационная безопасность	Воронеж: Воронежский Государственный Аграрный Университет им. Императора Петра Первого	2015	<a href="http://www.iprbookshop.ru/72672.html">http://www.iprbookshop.ru/72672.html</a>
Нестеров С.А.,	Основы информационной безопасности	Санкт-Петербург: Санкт-Петербургский политехнический университет Петра Великого	2014	<a href="http://www.iprbookshop.ru/43960.html">http://www.iprbookshop.ru/43960.html</a>

Басалова, Г. В.	Основы криптографии	Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа	2020	<a href="http://www.iprbookshop.ru/89455.html">http://www.iprbookshop.ru/89455.html</a>
-----------------	---------------------	--	------	---

#### 6.1.2 Дополнительная учебная литература

Кикин А. Б.	Информационная безопасность. Основы криптографии	СПб.: СПбГУПТД	2019	<a href="http://publish.sutd.ru/tp_ext_inf_publish.php?id=201932">http://publish.sutd.ru/tp_ext_inf_publish.php?id=201932</a>
Кикин А. Б.	Информационная безопасность	СПб.: СПбГУПТД	2015	<a href="http://publish.sutd.ru/tp_ext_inf_publish.php?id=2809">http://publish.sutd.ru/tp_ext_inf_publish.php?id=2809</a>
Кикин А. Б.	Информационная безопасность	СПб.: СПбГУПТД	2014	<a href="http://publish.sutd.ru/tp_ext_inf_publish.php?id=1695">http://publish.sutd.ru/tp_ext_inf_publish.php?id=1695</a>
Кикин А.Б.	Хранение и защита компьютерной информации	СПб.: СПбГУПТД	2015	<a href="http://publish.sutd.ru/tp_ext_inf_publish.php?id=2807">http://publish.sutd.ru/tp_ext_inf_publish.php?id=2807</a>

#### 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](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

MicrosoftOfficeProfessional  
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
Учебная аудитория	Специализированная мебель, доска