# D:\15.04.04-1\smike_2021-04-26_18-08-13\image--076.jpg

# 1. Цели освоения дисциплины

Целями освоения дисциплины является формирование у обучающихся определенного ООП (п. 5. Общей характеристики ООП) состава компетенций для подготовки к профессиональной деятельности.

|  |  |  |
| --- | --- | --- |
| **Код компетенции** | **Наименование компетенции** | **Составляющие результатов освоения (дескрипторы компетенции)** |
| **Код** | **Наименование** |
| УК(У)-2 | Способен управлять проектом на всех этапах его жизненного цикла | УК(У)-2.В1 | Способностью определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений |
| УК(У)-2.У1 | Определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений |
| УК(У)-2.З1 | Методиками определения задач в рамках поставленной цели и выбором оптимальных способов их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений |
| ПК(У)-1 | способность разрабатывать технические задания на модернизацию и автоматизацию действующих производственных и технологических процессов и производств, технических средств и систем автоматизации, управления, контроля, диагностики и испытаний, новые виды продукции, автоматизированные и автоматические технологии ее производства, средства и системы автоматизации, управления процессами, жизненным циклом продукции и ее качеством | ПК(У)-1.В1 | Владение опытом составления технического задания на разработку схемотехнических и алгоритмических решений, выбор аппаратных средств для систем управления технологическим процессом  |
| ПК(У)-1.У1 | Разрабатывать функциональную, логическую и техническую организацию автоматизированных и автоматических производств, их элементов, технического, алгоритмического и программного обеспечения на базе современных методов, средств и технологий проектирования |
| ПК(У)-1.З1 | Знание основных схемотехнических, алгоритмических и аппаратных решений в системах управления автоматизированных комплексов цифровых производств |

# 2. Место дисциплины (модуля) в структуре ООП

Дисциплина относится к базовой части Блока 1 учебного плана образовательной программы.

# 3. Планируемые результаты обучения по дисциплине

После успешного освоения дисциплины будут сформированы результаты обучения:

|  |  |
| --- | --- |
| **Планируемые результаты обучения по дисциплине** | **Компетенции** |
| **Код** | **Наименование** |
| РД-1 | Знание методов определения задач в рамках поставленной цели и выбором оптимальных способов их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений | УК(У)-2 |
| РД-2 | Умение определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений | УК(У)-2 |
| РД-3 | Владение способностью определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений | УК(У)-2 |
| РД-4 | Знание методов и средств повышения безопасности, технологичности и устойчивости технических средств и технологических процессов; принципы рационального и безопасного использования природных ресурсов, энергии и материалов | УК(У)-2 |
| РД-5 | Умение применять принципы обеспечения экологической безопасности при решении практических задач в области автоматизации технических процессов и производств, управления жизненным циклом продукции и ее качеством; разрабатывать мероприятия по повышению безопасности и экономичности производственной деятельности | УК(У)-2 |
| РД-6 | Владение разработкой проектных решений по обеспечению безопасности производственного и научного персонала | УК(У)-2 |
| РД-7 | Знание информационных и программных средств контроля, диагностики, испытаний и управления при изменении действия внешних факторов | ПК(У)-1 |
| РД-8 | Умение обеспечивать информационную безопасность автоматизированных систем | ПК(У)-1 |
| РД-9 | Владение методами обеспечения информационной безопасности и жизнестойкости цифровых систем | ПК(У)-1 |

# Оценочные мероприятия текущего контроля и промежуточной аттестации представлены в календарном рейтинг-плане дисциплины.

# 4. Структура и содержание дисциплины

**Основные виды учебной деятельности**

|  |  |  |  |
| --- | --- | --- | --- |
| **Разделы дисциплины** | **Формируемый результат обучения по дисциплине** | **Виды учебной деятельности** | **Объем времени, ч.** |
| Раздел 1. Основы систем промышленной информационной безопасности | РД-1, РД-2, РД-3, РД-4, РД-5, РД-6, РД-7, РД-8, РД-9 | Лекции | 4 |
| Практические занятия | 8 |
| Лабораторные занятия | 12 |
| Самостоятельная работа | 30 |
| Раздел 2. Алгоритмы шифрования. Атаки на алгоритмы шифрования | РД-1, РД-2, РД-3, РД-4, РД-5, РД-6, РД-7, РД-8, РД-9 | Лекции | 4 |
| Практические занятия | 8 |
| Лабораторные занятия | 12 |
| Самостоятельная работа | 30 |

Содержание разделов дисциплины:

**Раздел 1. Основы систем промышленной информационной безопасности**

Основные понятия информационной безопасности (ИБ). Основные задачи системы ИБ. Виды информационных угроз. Компьютерные преступления. Защита информации. Современные системы идентификации и аутентификации пользователей

**Темы лекций:**
1. Основные понятия информационной безопасности
2. Информационная безопасность АСУ ТП

**Темы практических занятий:**
1. Аутентификация. Количественная оценка стойкости парольной защиты
2. Реализация политики информационной безопасности

**Темы лабораторных работ:**
1. Аутентификация. Количественная оценка стойкости парольной защиты
2. Формирование эшелонированной защиты АСУ ТП
3. Реализация политики информационной безопасности

**Раздел 2. Алгоритмы шифрования. Атаки на алгоритмы шифрования**

Классификация алгоритмов шифрования. Основные определения. Структура алгоритмов симметричного шифрования. Алгоритмы на основе сети Фейстеля. Расширенная сеть Фейстеля. Алгоритмы на основе подстановочно-перестановочных сетей. Алгоритмы со структурой «квадрат». Алгоритмы с нестандартной структурой. Режимы работы алгоритмов. Электронная кодовая книга (ECB). Сцепление блоков шифра (CBC). Обратная связь по шифртексту (CFB). Обратная связь по выходу (OFB). Основные характеристики и структура DES. Описание шифрования DES. Криптостойкость алгоритма DES

**Темы лекций:**
1. Алгоритмы шифрования
2. Атаки на алгоритмы шифрования

**Темы практических занятий:**
1. Классические криптографические системы
2. Ассиметричные алгоритмы шифрования данных. Алгоритм RSA

**Темы лабораторных работ:**
1. Классические криптографические системы
2. Ассиметричные алгоритмы шифрования данных. Алгоритм RSA
3. Электронная цифровая подпись

# 5. Организация самостоятельной работы студентов

Самостоятельная работа студентов при изучении дисциплины (модуля) предусмотрена в следующих видах и формах:

- Работа с лекционным материалом, поиск и обзор литературы и электронных источников информации по индивидуально заданной проблеме курса
- Изучение тем, вынесенных на самостоятельную проработку
- Поиск, анализ, структурирование и презентация информации
- Подготовка к лабораторным работам, к практическим и семинарским занятиям
- Выполнение курсовой работы или проекта, работа над междисциплинарным проектом
- Анализ научных публикаций по заранее определенной преподавателем теме
- Подготовка к оценивающим мероприятиям

# 6. Учебно-методическое и информационное обеспечение дисциплины

**6.1. Учебно-методическое обеспечение**

**Основная литература**
1. Адаменко, М. В. Основы классической криптологии: секреты шифров и кодов / М. В. Адаменко. — 2-е изд., испр. и доп. — Москва : ДМК Пресс, 2016. — 296 с. — ISBN 978-5-97060-166-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/82817 (дата обращения: 10.07.2019). — Режим доступа: для авториз. пользователей.
2. Коржик, В. И. Основы криптографии : учебное пособие / В. И. Коржик, В. А. Яковлев. — Санкт-Петербург : Интермедия, 2016. — 296 с. — ISBN 978-5-89160-097-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/90264 (дата обращения: 10.07.2019). — Режим доступа: для авториз. пользователей.

**Дополнительная литература**
1. Информационный мир XXI века. Криптография – основа информационной безопасности / под редакцией Э. А. Болелова. — 2-е изд. — Москва : Дашков и К, 2018. — 126 с. — ISBN 978-5-394-03031-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103793 (дата обращения: 10.07.2019). — Режим доступа: для авториз. пользователей/

**6.2. Информационное и программное обеспечение**

Internet-ресурсы (в т.ч. в среде LMS MOODLE и др. образовательные и библиотечные ресурсы):

1. [Электронный ресурс] Электронная библиотечная система «Лань». – Режим доступа: URL. – <https://e.lanbook.com/>

2. [Электронный ресурс] Электронная библиотечная система «Консультант студента» – Режим доступа: URL. – <http://www.studentlibrary.ru/>

3. [Электронный ресурс] Электронная библиотечная система «Юрайт» – Режим доступа: URL. – <http://www.studentlibrary.ru/>

4. [Электронный ресурс] Электронная библиотечная система «Znanium» – Режим доступа: URL. – http://znanium.com/

Лицензионное программное обеспечение (в соответствии с **Перечнем лицензионного программного обеспечения ТПУ)**:

1. Acrobat Reader DC and Runtime Software Distribution Agreement
2. Webex Meetings
3. Visual C++ Redistributable Package
4. MatLab, компания The MathWorks

# 7. Особые требования к материально-техническому обеспечению дисциплины

|  |  |  |
| --- | --- | --- |
| **№** | **Наименование специальных помещений** | **Наименование оборудования** |
| 1 | Аудитория для проведения учебных занятий всех типов, курсового проектирования, консультаций, текущего контроля и промежуточной аттестации Учебный корпус № 10, 415, 634028 РФ, Томская обл., г.Томск, пр-кт Ленина, д.2 | Компьютер - 1 шт.;Проекторы - 1 шт. Макет космического аппарата ГЛОНАСС-К в масштабе 1:10 - 1 шт.;Макет космического аппарата МОЛНИЯ в масштабе 1:10 - 1 шт.;Макет космического аппарата ЛУЧ в масштабе 1:10 - 1 шт.; Доска аудиторная настенная - 1 шт.;Шкаф для одежды - 1 шт.;Шкаф для документов - 4 шт.;Тумба подкатная - 5 шт.;Стул - 30 шт.;Стол лабораторный - 5 шт.;Стол для преподавателя - 1 шт.;Стол аудиторный - 16 шт.;Кресло - 1 шт.; |
| 2 | Аудитория для проведения учебных занятий всех типов, курсового проектирования, консультаций, текущего контроля и промежуточной аттестации (учебная лаборатория) Учебный корпус № 10, 103, 634028 РФ, Томская обл., г.Томск, пр-кт Ленина, д.2 | Компьютер - 5 шт.;Проекторы - 1 шт. Стенд "Современные средства автоматизации" - 1 шт.;Демо система Екш-ПЗ для демонстрации и обучения - 1 шт.;Унифицированный аппаратно-программный стенд - 1 шт.;Демо система Foxboro Evo для демонстрации и обучения - 1 шт.; Кресло - 1 шт.;Тумба стационарная - 3 шт.;Стул - 2 шт.;Парта - 2 шт.; |
| 3 | Аудитория для проведения учебных занятий всех типов, курсового проектирования, консультаций, текущего контроля и промежуточной аттестации (научная лаборатория) Учебный корпус № 10, 101А, 634028 РФ, Томская обл., г.Томск, пр-кт Ленина, д.2 |  Комплект Робот DARwln-OP Deluxe Edition - 1 шт.;Учебная система Robotino - 1 шт.;Осциллограф OWON SDS 7102V - 1 шт.;Человекоподобный робот ROBOTIS-OP 2 - 3 шт.;Мобильный робот LEGO MINDSTORMS NXT 2.0 - 1 шт.;Мультиметр MS8240B - 2 шт.;Робот BioLoid Comprehensive - 1 шт.;Робототехнический набор-конструктор Bioloid Premium Kit - 2 шт.;Робототехнический образовательный комплекс - 1 шт.; Стол аудиторный - 1 шт.;Шкаф для документов - 2 шт.;Тумба стационарная - 1 шт.;Тумба подкатная - 1 шт.;Стол компьютерный - 46 шт.; |
| 4 | Аудитория для проведения учебных занятий всех типов, курсового проектирования, консультаций, текущего контроля и промежуточной аттестации (компьютерный класс) Учебный корпус № 10, 106, 634028 РФ, Томская обл., г.Томск, пр-кт Ленина, д.2 | Компьютер - 9 шт. Информационный стенд № 1 - DKC "Алюминиевые кабельные каналы" - 1 шт.;,Источник питания NES-100-12 - 1 шт.;Специализированный учебно-научный комплекс интегрированных компьютерных систем - 1 шт.;Стенд № 6 "Металлокорпуса для электрощитов" - 1 шт.;Стенд № 5 "Силовое оборудование и кнопки" - 1 шт.;Стенд № 2 "Клеммное обеспечение автоматизированных систем" - 1 шт.;Стенд № 4 "Коммутационная модульная аппаратура (EKF electronica) - 1 шт.;Стенд № 3 "Силовые автоматические выключатели (EKF) - 1 шт.; Кресло - 14 шт.;Тумба стационарная - 2 шт.;Стул - 7 шт.;Стол аудиторный - 15 шт.; |
| 5 | Аудитория для проведения учебных занятий всех типов, курсового проектирования, консультаций, текущего контроля и промежуточной аттестации (компьютерный класс) Учебный корпус № 10, 108, 634028 РФ, Томская обл., г.Томск, пр-кт Ленина, д.2 | Компьютер - 15 шт. Учебный комплект на базе промыш.микропроцессорного контроллера Simatic S7--200 - 1 шт.; Доска аудиторная настенная - 1 шт.;Стол аудиторный - 24 шт.; |
| 6 | Аудитория для проведения учебных занятий всех типов, курсового проектирования, консультаций, текущего контроля и промежуточной аттестации (компьютерный класс) Учебный корпус № 10, 109, 634028 РФ, Томская обл., г.Томск, пр-кт Ленина, д.2 | Компьютер - 15 шт. Доска аудиторная настенная - 1 шт.;Стол аудиторный - 6 шт.; |



**Лист изменений рабочей программы дисциплины[[1]](#footnote-1):**

|  |  |  |
| --- | --- | --- |
| **Учебный год** | **Содержание /изменение** | **Обсуждено на заседании ОАР (протокол)** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. *Ежегодное обновление программы с учетом развития науки, культуры, экономики, техники и технологий, социальной сферы.* [↑](#footnote-ref-1)