

НПОУ «ЯКУТСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

УТВЕРЖДАЮ  
Директор НПОУ «ЯКИТ»  
Л.Н. Цой  
«27» августа 2021 г.



## РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

### ОП.06 Основы информационной безопасности

Специальность: 10.02.01 Организация и технология защиты информации

**Профиль подготовки:** технический

**Квалификация** техник по защите информации

**Форма обучения** очная

**Год набора** 2021

Якутск, 2021

# 1. ПАСПОРТ РАБОЧЕЙ УЧЕБНОЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

## 1.1. Область применения рабочей учебной программы

Учебная программа дисциплины является частью образовательной программы в соответствии с ФГОС по специальности **10.02.01 Организация и технология защиты информации**

## 1.2. Место дисциплины в структуре программы подготовки специалистов среднего звена:

П. Профессиональный цикл

ОП. Общепрофессиональные дисциплины

ОП.06. Основы информационной безопасности

## 1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины:

В результате освоения дисциплины студент должен **уметь**:

- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- применять основные правила и документы системы сертификации Российской Федерации;
- классифицировать основные угрозы безопасности информации.

В результате освоения дисциплины студент должен **знать**:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- источники угроз информационной безопасности и меры по их предотвращению;
- жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности.

### Формируемые компетенции:

#### Общие компетенции

|       |  |
|-------|--|
| ОК 1. | Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности. |
| ОК 2. | Организовывать собственную деятельность, выбирать типовые методы и способы   |

|       |  |
|-------|--|
|       | выполнения профессиональных задач, оценивать их эффективность и качество.  |
| ОК 3. | Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.  |
| ОК 4. | Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития. |
| ОК 5. | Использовать информационно–коммуникационные технологии в профессиональной деятельности.  |
| ОК 6. | Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.   |
| ОК 7. | Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.  |
| ОК 8. | Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.    |
| ОК 9. | Ориентироваться в условиях частой смены технологий в профессиональной деятельности.  |

### Профессиональные компетенции

| Код     | Наименование видов профессиональной деятельности и профессиональных компетенций                  |
|---------|--|
| ПК 1.6. | Обеспечивать технику безопасности при проведении организационно-технических мероприятий.         |
| ПК 3.1  | Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах. |
| ПК 3.2  | Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.               |
| ПК 3.3  | Проводить регламентные работы и фиксировать отказы средств защиты.                               |
| ПК 3.4  | Выявлять и анализировать возможные угрозы информационной безопасности объектов.                  |

#### 1.4. Рекомендуемое количество часов на освоение программы дисциплины:

максимальной учебной нагрузки обучающегося 80 часов, в том числе:

обязательной аудиторной учебной нагрузки обучающегося 64 часов;

самостоятельной работы обучающегося 16 часов.

## 2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 2.1. Виды учебной работы и объём учебных часов

| <b>Вид учебной работы</b>                                   | <b>Объём, ч</b> |
|---|-----------------|
| Максимальная учебная нагрузка                               | 80              |
| Обязательная аудиторная учебная нагрузка, в том числе       | 64              |
| практические и семинарские занятия                          | 32              |
| контрольная работа  | -               |
| Самостоятельная работа обучающегося                         | 16              |
| Промежуточная аттестация в форме дифференцированного зачёта |                 |

## 2.2. Тематический план и содержание учебной дисциплины ОП.1 Основы информационной безопасности

| Наименование разделов и тем  | Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект) (если предусмотрены) |  | Объем часов | Уровень освоения |
|--|--|--|-------------|------------------|
| 1  | 2  |  | 3           | 4                |
| Раздел 1   | Введение   |  |             |                  |
| Тема 1.1. Информация. Информационные системы                         | 1  | Информация. Информационные системы                         |             |                  |
|  |  | Лекции   | 1           |                  |
|  |  | Лабораторные работы  | 1           |                  |
|  |  | Контрольные работы   | -           |                  |
|  |  | Самостоятельная работа студента                            | 1           |                  |
| Раздел 2.  | Информационная безопасность  |  |             |                  |
| Тема 2.1. Современная ситуация в области информационной безопасности | 1  | Современная ситуация в области информационной безопасности |             |                  |
|  |  | Лекции   | 1           |                  |
|  |  | Лабораторные работы  | 1           |                  |
|  |  | Контрольные работы   |             |                  |
|  |  | Самостоятельная работа студента                            | 1           |                  |
| Тема 2.2. Основные виды и источники атак на информацию               | 2  | Основные виды и источники атак на информацию               |             |                  |
|  |  | Лекции   | 1           |                  |

|   |   |   |   |  |
|---|---|---|---|--|
|   |   | Лабораторные работы                             |   |  |
|   |   | Контрольные работы                              | 1 |  |
|   |   | Самостоятельная работа студента                 | 1 |  |
| <b>Тема 2.3. Угроза безопасности информации</b>           | 3 | <b>Угроза безопасности информации</b>           |   |  |
|   |   | Лекции  | 1 |  |
|   |   | Лабораторные работы                             | 1 |  |
|   |   | Контрольные работы                              |   |  |
|   |   | Самостоятельная работа студента                 | 1 |  |
| <b>Тема 2.4. Факторы угроз безопасности информации</b>    | 4 | <b>Факторы угроз безопасности информации</b>    |   |  |
|   |   | Лекции  | 1 |  |
|   |   | Лабораторные работы                             | 1 |  |
|   |   | Контрольные работы                              |   |  |
|   |   | Самостоятельная работа студента                 | 1 |  |
| <b>Тема 2.5. Критерии и нормы безопасности информации</b> | 5 | <b>Критерии и нормы безопасности информации</b> |   |  |
|   |   | Лекции  | 2 |  |
|   |   | Лабораторные работы                             | 2 |  |
|   |   | Контрольные работы                              |   |  |
|   |   | Самостоятельная работа студента                 | 1 |  |
| <b>Тема 2.6. Категории</b>                                | 6 | <b>Категории информационной безопасности</b>    |   |  |

|   |   |   |   |     |
|---|---|---|---|-----|
| информационной безопасности                           |   |   |   |     |
|   |   | Лекции  | 2 |     |
|   |   | Лабораторные работы   | 2 |     |
|   |   | Контрольные работы  |   |     |
|   |   | Самостоятельная работа студента   | 1 |     |
| Тема 2.7. Жизненные циклы конфиденциальной информации | 7 | <b>Жизненные циклы конфиденциальной информации</b>                            |   |     |
|   |   | Лекции  | 2 |     |
|   |   | Лабораторные работы   | 2 |     |
|   |   | Контрольные работы  |   |     |
|   |   | Самостоятельная работа студента   | 1 |     |
| Раздел 3.   |   | <b>Современные средства и способы обеспечения информационной безопасности</b> |   |     |
| Тема 3.1. Абстрактные модели защиты информации        | 1 | <b>Абстрактные модели защиты информации</b>                                   |   | 1,3 |
|   |   | Лекции  | 2 |     |
|   |   | Лабораторные работы   | 2 |     |
|   |   | Контрольные работы  |   |     |
|   |   | Самостоятельная работа студента   | 1 |     |
| Тема 3.2. Наиболее распространенные методы взлома     | 2 | <b>Наиболее распространенные методы взлома</b>                                |   | 1   |
|   |   | Лекции  | 2 |     |
|   |   | Лабораторные работы   | 2 |     |

|  |           |  |   |              |
|--|-----------|--|---|--------------|
|  |           | Контрольные работы                                   |   |              |
|  |           | Самостоятельная работа студента                      |   |              |
| <b>Тема 3.3. Средства и способы обеспечения информационной</b> | <b>1</b>  | <b>Средства и способы обеспечения информационной</b> |   | <b>1,2,3</b> |
|  |           | Лабораторные работы                                  | 1 |              |
|  |           | Контрольные работы                                   | 1 |              |
|  |           | Самостоятельная работа студента                      | 1 |              |
| <b>Тема 3.7. Методы антивирусной защиты информации</b>         | <b>6.</b> | <b>Методы антивирусной защиты информации</b>         |   |              |
|  |           | Лекции   | 1 |              |
|  |           | Лабораторные работы                                  | 2 |              |
|  |           | Контрольные работы                                   |   |              |
|  |           | Самостоятельная работа студента                      | 1 |              |
| <b>Раздел 4.</b>   |           | <b>Защита информации в информационных системах</b>   |   |              |
| <b>Тема 4.1. Вычислительные сети и защита информации</b>       | <b>1</b>  | <b>Вычислительные сети и защита информации</b>       |   |              |
|  |           | Лекции   | 1 |              |
|  |           | Лабораторные работы                                  | 1 |              |
|  |           | Контрольные работы                                   |   |              |
|  |           | Самостоятельная работа студента                      | 2 |              |
| <b>Тема 4.2. Защита локальных сетей и операционных систем</b>  | <b>2</b>  | <b>Защита локальных сетей и операционных систем</b>  |   |              |
|  |           | Лекции   | 1 |              |
|  |           | Лабораторные работы                                  | 1 |              |
|  |           | Контрольные работы                                   |   |              |

|  |  |   |   |  |
|--|--|---|---|--|
|  | Самостоятельная работа студента                                      |   |   |  |
| Тема 4.3. Проблемы защиты информации в Интернет.<br>Рекомендации по защите информации в Интернет | 1.   | <b>Проблемы защиты информации в Интернет. Рекомендации по защите информации в Интернет</b>            |   |  |
|  | Лекции   |   | 1 |  |
|  | Лабораторные работы  |   | - |  |
|  | Контрольные работы   |   |   |  |
|  | Самостоятельная работа студента                                      |   | 1 |  |
| Тема 4.4.<br>Информационная безопасность в Intranet  | 2.   | <b>Информационная безопасность в Intranet.</b>  |   |  |
|  | Лекции   |   | 1 |  |
|  | Лабораторные работы  |   | 1 |  |
|  | Контрольные работы   |   |   |  |
|  | Самостоятельная работа студента                                      |   | 2 |  |
| Раздел 4.  | <b>Нормативно – правовое обеспечение информационной безопасности</b> |   |   |  |
| Тема 4.1. Основные правила и документы системы сертификации РФ                                   | 1  | <b>Основные правила и документы системы сертификации РФ</b>   |   |  |
|  | Лекции   |   | 1 |  |
|  | Лабораторные работы  |   | - |  |
|  | Контрольные работы   |   |   |  |
|  | Самостоятельная работа студента                                      |   | 2 |  |
| Тема 4.2. Нормативно-правовое обеспечение информационной безопасности программно-аппаратными     | 2  | <b>Нормативно- правовое обеспечение информационной безопасности программно-аппаратными средствами</b> |   |  |
|  | Лекции   |   | 1 |  |
|  | Лабораторные работы  |   | 1 |  |
|  | Контрольные работы   |   |   |  |

|   |                                 |  |    |  |
|---|---------------------------------|--|----|--|
| средствами  | Самостоятельная работа студента |  | 1  |  |
| Тема 4.3. Нормативно-правовое обеспечение информационной безопасности инженерно-техническими средствами | 3                               | <b>Нормативно-правовое обеспечение информационной безопасности инженерно-техническими средствами</b> |    |  |
|   |                                 | Лекции   | 1  |  |
|   |                                 | Лабораторные работы  | 1  |  |
|   |                                 | Контрольные работы   |    |  |
|   |                                 | Самостоятельная работа студента  | 1  |  |
| Самостоятельная работа обучающихся  |                                 |  | 24 |  |
| <b>Всего:</b>   |                                 |  | 72 |  |

1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

### **3. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ**

#### **3.1. Требования к минимальному материально-техническому обеспечению**

Реализация дисциплины проводится в учебной лекционной аудитории; в компьютерных кабинетах, лабораториях.

Оборудование лабораторий и рабочих мест лабораторий: рабочие места, проектор, ПК, учебное ППО. Состав программного обеспечения: операционная система с графической операционной оболочкой (Microsoft Windows, GNU/Linux), интегрированный пакет прикладных программ офисного назначения и другие. Дополнительно: в составе программного обеспечения файлового менеджера, архиватора, программы просмотра графических изображений с конвертором форматов, растрового и векторного графических. Специальные помещения должны представлять собой учебные аудитории для проведения учебных занятий всех типов, предусмотренных образовательной программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы, мастерские и лаборатории, оснащенные оборудованием, техническими средствами обучения и материалами, учитывающими требования ФГОС.

Помещения для самостоятельной работы обучающихся должны быть оснащены компьютерной техникой с возможностью подключения к сети «Интернет» обеспечением доступа в электронную информационно - образовательную среду образовательной организации (при наличии). В случае применения электронного обучения, дистанционных образовательных технологий допускается замена специально оборудованных помещений их виртуальными аналогами, позволяющими обучающимся осваивать УК и ПК.

Образовательная организация должна быть обеспечена необходимым комплектом лицензионного программного обеспечения, состав которого определяется в рабочих программах учебных предметов, курсов, дисциплин (модулей) и подлежит ежегодному обновлению.

### 3.2. Информационное обеспечение обучения

#### Основная литература\*

1 Информационная безопасность: учеб./под ред. В.П.,Мельникова.- М.: Кнорус, 2018. –Рек. ФИРО

#### Дополнительная литература

2. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза: монография, Смирнов А.А., ЮНИТИ-ДАНА; Закон и право, Москва, 2019

3. Защита информации в компьютерных системах и сетях, Шаньгин В.Ф., ДМК Пресс, Москва, 2017

Методы и средства инженерно-технической защиты информации: учебное пособие, Аверченков В.И., Рытов М.Ю., Кувыклин А.В., Гайнулин Т.Р., ФЛИНТА, Москва, 2018

#### Интернет- ресурсы

1 Exponenta.ru Компания «АХОФТ»

2 Wikipedia.org Компания «Vikipedia Foundation»

## 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

**Контроль и оценка** результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

| Результаты обучения<br>(освоенные умения, усвоенные знания)                               | Формы и методы контроля и оценки результатов обучения  |
|---|--|
| Уметь классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности | Промежуточная аттестация: практическое задание;<br>Текущий контроль: контрольная работа, лабораторная работа |
| Уметь применять основные правила и документы системы сертификации Российской Федерации    | Промежуточная аттестация: практическое задание;<br>Текущий контроль: контрольная работа, лабораторная работа |
| Уметь классифицировать основные угрозы безопасности информации                            | Промежуточная аттестация: практическое задание;<br>Текущий контроль: контрольная работа, лабораторная работа |

|  |   |
|--|---|
| <p>Знать сущность и понятие информационной безопасности, характеристику ее составляющих</p>          | <p>Промежуточная аттестация:<br/>практическое задание;<br/><br/>Текущий контроль: контрольная работа, лабораторная работа</p> |
| <p>Знать место информационной безопасности в системе национальной безопасности страны</p>            | <p>Промежуточная аттестация:<br/>практическое задание;<br/><br/>Текущий контроль: контрольная работа, лабораторная работа</p> |
| <p>Знать источники угроз информационной безопасности и меры по их предотвращению</p>                 | <p>Промежуточная аттестация:<br/>практическое задание;<br/><br/>Текущий контроль: контрольная работа, лабораторная работа</p> |
| <p>Знать жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи</p> | <p>Промежуточная аттестация:<br/>практическое задание;<br/><br/>Текущий контроль: контрольная работа, лабораторная работа</p> |
| <p>Знать современные средства и способы обеспечения информационной безопасности</p>                  | <p>Текущий контроль: тестирование, контрольная работа</p>   |



|  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |