НПОУ «ЯКУТСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

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

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ПМ.01. УЧАСТИЕ В ПЛАНИРОВАНИИ И ОРГАНИЗАЦИИ РАБОТ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ОБЪЕКТА

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

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности / профессии 10.02.01 Организация и технология защиты информации

(код и наименование специальности / профессии)

Организация-разработчик:
НПОУ «Якутский колледж инновационных технологий»

Разработчики:

Тронь Татьяна Александровна, преподаватель
Ф.И.О., ученая степень, звание, должность

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Область применения рабочей программы

Рабочая программа профессионального модуля является частью образовательной программы в соответствии с ФГОС СПО по специальности / профессии 10.02.01 Организация и технология защиты информации

(код и наименование специальности / профессии)

1.2. Место профессионального модуля в структуре образовательной программы:

ПК 1.1 Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации.

ПК 1.2 Участвовать в разработке программ и методик организации защиты информации на объекте.

ПК 1.3 Осуществлять планирование и организацию выполнения мероприятий по защите информации.

ПК 1.4 Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности.

ПК 1.5 Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации.

ПК 1.6 Обеспечить технику безопасности при проведении организационно-технических мероприятий.

ПК 1.7 Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите.

ПК 1.8 Проводить контроль соблюдения персоналом требований режима защиты информации.

ПК 1.9 Участвовать в оценке качества защиты объекта.

1.3. Цели и задачи профессионального модуля – требования к результатам освоения профессионального модуля:

В результате освоения профессионального модуля обучающийся должен иметь практический опыт:

-использование физических средств защиты информации;

-применение физических средств контроля доступа на объект;

-ведение текущей работы исполнителей с конфиденциальной информацией.

В результате освоения профессионального модуля обучающийся должен уметь:

- организовывать охрану персонала, территорий, зданий, помещений и продукции организаций;

-пользоваться аппаратурой систем контроля доступа;

-выделять зоны доступа по типу и степени конфиденциальности работ;

-определять порядок организации и проведения рабочих совещаний;

-использовать методы защиты информации в рекламной и выставочной деятельности;

-использовать критерии подбора и расстановки сотрудников подразделений защиты информации;

-организовывать работу с персоналом, имеющим доступ к конфиденциальной информации;

-проводить инструктаж персонала по организации работы с конфиденциальной информацией;

-контролировать соблюдение персонала требований режима защиты информации.

В результате освоения профессионального модуля обучающийся должен знать:

-виды и способы охраны объекта;

-особенности охраны персонала организации;

-основные направления и методы организации режима и охраны объекта;

-разрешительную систему доступа к конфиденциальной информации;

-принципы действия аппаратуры систем контроля доступа;

-принципы построения и функционирования биометрических систем безопасности;

-требования и порядок реализации режимных мер в ходе подготовки и проведения совещаний по конфиденциальным вопросам и переговоров;

-требования режима защиты информации при приеме в организации посетителей;

-организацию работы при осуществлении международного сотрудничества;

-требования режима защиты информации в процессе рекламной деятельности;

-требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати;

-задачи, функции и структуру подразделений защиты информации;

-принципы, методы и технологию управления подразделений защиты информации;

-порядок оформления допуска лиц к конфиденциальным сведениям;

-методы проверки персонала пот защите информации;

-процедуру служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией.

ПК и ОК, которые актуализируются при изучении профессионального модуля:

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.

ОК 10. Применять математический аппарат для решения профессиональных задач.

ОК 11. Оценивать значимость документов, применяемых в профессиональной деятельности.

ОК 12. Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность.

1.4. Количество часов на освоение профессионального модуля:

Максимальной учебной нагрузки обучающегося 616 часов, в том числе:

- аудиторной учебной работы обучающегося (обязательных учебных занятий) 390 часов
- внеаудиторной (самостоятельной) учебной работы обучающегося 163 часов;

− учебной и производственной практики (для профессионального модуля) 288 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Объем профессионального модуля и виды учебной работы

Вид учебной работы	**Объем часов**
Максимальная учебная нагрузка (всего)	554
Аудиторная учебная работа (обязательные учебные занятия) (всего)	390
в том числе:	
лабораторные занятия (если предусмотрено)	106
в том числе в форме практической подготовки (если предусмотрено)	-
практические занятия (если предусмотрено)	142
в том числе в форме практической подготовки (если предусмотрено)	-
контрольные работы (если предусмотрено)	-
курсовая работа (проект) (если предусмотрено)	
Внеаудиторная (самостоятельная) учебная работа обучающегося (всего)	163
в том числе:	
самостоятельная работа над курсовой работой (проектом) (если предусмотрено)	-
Учебная и производственная практика (для профессионального модуля)	72
Промежуточная аттестация в форме: _____Экзамен_____	

2.2. Тематический план и содержание профессионального модуля

Наименование разделов и тем	Содержание учебного материала, практические занятия, самостоятельная работа обучающихся, домашняя работа		Объем часов	Уровень освоения
МДК.1.1 Обеспечение организации систем безопасности предприятия			**173**	
Раздел 1. Основные понятия безопасности предприятия			**48**	
Тема 1.1. Основные понятия безопасности предприятия	**Содержание учебного материала**		**4**	
	1.	Понятие и содержание безопасности предприятия. Цель обеспечение безопасности предприятия.	2	3
	2.	Предмет, объекты и субъекты безопасности предприятия.	2	3
	Практические занятия		**8**	
	1.	Концепция безопасности предприятия.	4	
	2.	Структура концепции безопасности предприятия. Основные положения.	4	
	Самостоятельная работа		**10**	
	1.	Подготовить доклад на тему: Средства и методы обеспечения безопасности предприятия. Критерии безопасности предприятии.	10	
Тема 1.2. Виды угроз безопасности предприятия	**Содержание учебного материала**		**8**	
	1.	Понятие угроз безопасности предприятия и их классификация.	4	3
	2.	Сущность и содержание внутренних и внешних угроз безопасности предприятия.	2	3
	3.	Основные виды защищаемой информации.	2	3
	Практические занятия		**8**	
	1.	Общая классификация охраняемой информации.	4	

	2.	Выделение категорий деловой информации.	4	
	Самостоятельная работа		**10**	
	1.	Подготовить доклад на тему: Определение и содержание наиболее важных показателей безопасности предприятии. Построение эффективной системы безопасности предприятия.	10	
Раздел 2. Уязвимости информации			**33**	
Тема 2.1. Методы и модели оценки уязвимости информации	**Содержание учебного материала**		**2**	
	1.	Эмпирический подход к оценке уязвимости информации.	2	3
	Практические занятия		**2**	
	1.	Практическая реализация модели «угроза –защита»	2	
	Самостоятельная работа		**10**	
	1.	Подготовить доклад на тему: Государственная информационная политика. Проблемы информационной войны.	10	
Тема 2.2. Оценки уязвимости информации	**Содержание учебного материала**		**2**	
	1.	Определение методики выявление уязвимостей объекта.	2	3
	Практические занятия		**2**	
	1.	Рекомендации по использованию моделей оценки уязвимостей информации.	2	
	Самостоятельная работа		**10**	
	1.	Подготовить доклад на тему: Проблемы информационной безопасности в сфере государственного и муниципального	10	

		управления.		
Раздел 3. Требование к защите информации			**38**	
Тема 3.1. Методы определения требований к защите информации	**Содержание учебного материала**		**6**	
	1.	Требования к защите информации, обусловленные спецификой объекта защиты	2	3
	2.	Требования, определяемые структурой объекта защиты.	2	3
	3.	Требования к безопасности информационных систем в России.	2	3
	Практические занятия		**4**	
	1.	Классы защищенности средств вычислительной техники от несанкционированного доступа.	2	
	2.	Факторы, влияющие на требуемый уровень защиты информации объекта защиты.	2	
	Самостоятельная работа		**6**	
	1	Подготовить доклад на тему: Государственная система правового обеспечения защиты информации в РФ. Государственная информационная безопасность РФ.	6	
Тема 3.2. Функции и задачи защиты информации	**Содержание учебного материала**		**2**	
	1.	Общие положения. Методы формирования функций защиты.	2	3
	2.	Функции защиты. Состояние и функции системы защиты информации.	2	3
	Практические занятия		**2**	
	1.	Классы задач защиты информации.	2	
	Самостоятельная работа		**5**	
	1.	Подготовить доклад на тему: Законодательство в области информационной безопасности. Радиоэлектронные системы и	5	

		устройства защиты информации.		
Тема 3.3. Стратегии защиты информации.	**Содержание учебного материала**		**4**	
	1.	Организация защиты информации.	2	3
	2.	Уровень технологических схем обработки.	2	3
	Практические занятия		**4**	
	1.	Уровень структурно-организационного построения объекта обработки информации.	2	
	2.	Виды стратегии защиты информации.	2	
	Самостоятельная работа		**5**	
	1	Подготовить доклад на тему: Информационные инфекции. Политика и модели безопасности.	5	
Раздел 4. Организация охраны предприятия и физической защиты его объектов			**54**	
Тема 4.1. Организация охраны предприятия	**Содержание учебного материала**		**8**	
	1.	Основные объекты охраны предприятия. Виды и способы охраны объекта.	2	3
	2.	Основные задачи охраны объекта. Основные направления и методы организации режима и охраны объекта.	2	3
	3.	Задачи и функции службы безопасности предприятия.	2	3
	4.	Основные обязанности сотрудников подразделений охраны объекта. Особенности охраны персонала организации.	2	3
	Практические занятия		**6**	
	1.	Требования, предъявляемые к системе охраны.	2	

	2.	Организация охраны персонала, территорий, зданий, помещений и продукции организации.	2	
	3.	Разработка инструкций по организации охраны предприятия.	2	
	Самостоятельная работа		**5**	
	1.	Подготовить сообщение на темы: 1. Требования, связанные с размещением защищаемой информации. 2. Требования, обусловленные видом защищаемой информации. 3. Анализ существующих методик определение требований к защите информации. 4. Оценка состоянии безопасности ИС. 5. Методы защиты информации. 6. Средства защиты информации. 7. Требования к криптосистемам. Основные алгоритмы шифрования. 8. Цифровые подписи. Криптографические хеш-функции. 9. Криптографические генераторы случайных чисел. 10. Криптоанализ и атаки на криптосистемы. 11. Требования к архитектуре СЗИ. Построение СЗИ.	5	
Тема 4.2. Физическая защита предприятия	**Содержание учебного материала**		**14**	
	1.	Основные составляющие системы физической защиты предприятия. Особенности проектирования системы физической защиты предприятия.	2	3
	2.	Деятельность структурных подразделений службы безопасности предприятия.	4	3
	3.	Основные задачи инженерно-технической системы защиты информации. Разрешительная система доступа к конфиденциальной информации.	4	3
	4.	Принцип действия аппаратуры систем контроля доступа.	4	3
	Практические занятия		**16**	
	1.	Изучение работы аппаратуры систем контроля доступа.	2	

	2.	Выделение зон доступа по типу и степени конфиденциальностью работ.	2	
	3.	Классификация принципов инженерно-технической систем защиты информации.	2	
	4.	Классификация методов инженерно-технической системы защиты информации.	2	
	5.	Права, обязанности и ответственность сотрудников службы безопасности предприятия.	4	
	6.	Нештатные структуры службы безопасности предприятия.	4	
	Самостоятельная работа		**5**	
	1.	Подготовить сообщения на темы: 1. Требования, связанные с размещением защищаемой информации. 2. Требования, обусловленные видом защищаемой информации. 3. Анализ существующих методик определение требований к защите информации. 4. Оценка состоянии безопасности ИС. 5. Методы защиты информации.	5	
МДК.1.2 Организация работ подразделений защиты информации			172	
Раздел 1. Место и роль службы защиты информации в системе защиты информации			**70**	
Тема 1.1. Место и роль службы защиты информации в системе защиты информации	**Содержание учебного материала**		**6**	
	1.	Назначение службы защиты информации.	2	3
	2.	Место службы защиты информации как составляющая часть системы защиты информации.	2	3
	3	Служба защиты информации как составляющая часть системы защиты информации.	2	3
	Практические занятия		**6**	
	1.	Служба защиты информации как орган управления защитой информации.	2	
	2.	Статус службы защиты информации в структуре безопасности предприятии.	2	

	3.	Разработка организационно-правовых аспектов деятельности службы защиты информации.	2	
	Самостоятельная работа		**8**	
	1.	Подготовить сообщения на темы: Организационные задачи и функции службы защиты информации. Технологические задачи и функции службы защиты информации. Координационные задачи и функции службы защиты информации.	8	
Раздел 2. Принципы деятельности службы защиты информации			**76**	
Тема 2.1. Принципы и методы управления службой защиты информации	**Содержание учебного материала**		**21**	
	1.	Принципы и методы и технологии управления службой подразделений защиты информации. Принципы управления службой защиты информации.	7	3
	2.	Система методов управления. Взаимосвязь методов управления.	7	3
	3.	Необходимость комплексного и системного применения методов управления службой защиты информации.	7	3
	Самостоятельная работа		**10**	
	1.	Подготовить сообщения на темы: Организация труда сотрудников службы защиты информации. Организационные основы и принципы деятельности службы защиты информации.	10	
Тема 2.2. Организационные основы и принципы деятельности службы защиты информации	**Содержание учебного материала**		**21**	
	1.	Порядок создания службы защиты информации.	7	3
	2.	Структура и содержания положение о службе защиты информации.	7	3
	3.	Основные принципы организации и деятельности службы защиты информации.	7	3
	Практические занятия		**14**	
	1.	Состав и содержание других нормативных документов, регламентирующих деятельность	7	

		службы защиты информации.		
	2.	Экспертная оценка мероприятий по защите информации в службе защиты информации.	7	
	Самостоятельная работа		**10**	
		Подготовить сообщения на темы: Оценка производительности труда по результатам оптимизации процессов в службе защиты информации. Принципы и методы управления службой защиты информации.	10	
Раздел 3. Подбор, расстановка и обучение сотрудников службы защиты информации			**38**	
Тема 3.1. Подбор, расстановка и обучение сотрудников службы защиты информации.	**Содержание учебного материала**		**7**	
	1.	Общие и специфические требования, предъявляемые к сотрудникам службы защиты информации	7	3
	Практические занятия		**21**	
	1.	Критерии подбора и расстановки сотрудников подразделений защиты информации.	7	
	2.	Состав и характеристика процесса проектирования деятельности службы защиты информации.	7	
	3.	Формы повышения квалификации сотрудников. Подготовка кадрового резерва.	7	
	Самостоятельная работа		**10**	
	1.	Подготовить сообщения на темы: Общие и специфические требования, предъявляемые к сотрудникам службы защиты информации. Особенности подбора кадров.	10	
ПП.1.01 Производственная практика (по профилю специальности) **Виды работ:** 1. Использование физических средств защиты объекта.			180	

2. Применение физических средств контроля доступа на объекта. 3. Ведение текущей работы исполнительней с конфиденциальными документами.				
УП 1.01 Учебная практика **Виды работ:** Получение информации из открытых источников: 1. Использование Google для сбора информации; 2. Поиск информации о людях; 3. Получение информации о домене; 4. Автоматизирование процесса; 5. Упорядочение информации.			216	
Раздел ПМ 3. Работа персонала с конфиденциальной информацией.			**209**	
МДК 01.03 Организация работы персонала с конфиденциальной информацией.			**141**	
Тема 1. Особенности работы с конфиденциальной информацией.	**Содержание**		**8**	
	1.	Общие положение. Конфиденциальная информация.	2	1
	2.	Нормативная база конфиденциального делопроизводства.	2	2
	3.	Особенности работы с конфиденциальной информацией	2	
	Практические занятия		**2**	
	1.	Обработка персональных данных без использования средств автоматизации.		
Тема 2. Документирование конфиденциальной информации.	**Содержание**		**12**	
	1.	Особенности документирования конфиденциальной информации.	2	2
	2.	Учет бумажных носителей конфиденциальной информации и их проектов.	2	2

	3.	Документирование конфиденциальной информации	2	
	Практические занятия		**6**	
	1.	Разработка перечня конфиденциальной документированной информации.		
	2.	Определение степени ограничения доступа к документам.		
	3.	Использование отметки конфиденциальности при оформлении документов.		
Тема 3. Организация конфиденциального документооборота.	**Содержание**		**20**	
	1.	Учет и регистрация конфиденциальной документированной информации.	2	2
	2.	Учет и регистрация входящих конфиденциальных документов.	2	2
	3.	Учет и регистрация внутренних конфиденциальных документов.	2	2
	4.	Реестр конфиденциальной информации	2	
	5.	Ведение реестра конфиденциальной информации.	2	
	6.	Организация конфиденциального документооборота	2	
	7.	Обработка поступающих и внутренних конфиденциальных документов	2	
	8.	Исполнение и контроль за исполнением конфиденциальных документов	2	
	Практические занятия		**4**	
	1.	Обработка поступающих и внутренних конфиденциальных документов, их учет и регистрация.		
	2.	Учет и регистрация внутренних конфиденциальных документов.		

	Итоговое занятие за 6 семестр		**2**	
Тема 4. Разрешительная система доступа к конфиденциальной информации.	**Содержание**		**18**	
	1.	Регламент доступа к конфиденциальной информации.	2	2
	2.	Обязательство о неразглашении конфиденциальной информации.	2	2
	3.	Федеральный закон №152 "О персональных данных"	2	
	4.	Доступ к архивным конфиденциальным документам	2	
	5.	Органы государственной власти	2	
	6.	Служебная и коммерческая тайна	2	
	Практические занятия		**4**	
	1.	Доступ к информации, составляющей служебную, коммерческую, профессиональную тайны, секрет производства.		
	2	Доступ к информации, составляющей персональные данные		
	3.	Доступ к информации при ее предоставлении уполномоченным органам государственной власти.		
Тема 5. Составление номенклатуры дел, формирование и оформление конфиденциальных дел.	**Содержание**		**8**	
	1.	Номенклатура конфиденциальных дел	2	
	2	Учет конфиденциальных дел и составление номенклатуры конфиденциальных дел.	2	2
	Практические занятия		**4**	
	1.	Учет конфиденциальной информации формирование конфиденциальных дел.		

	2.	Формирование конфиденциальных дел.		
Тема 6. Подготовка конфиденциальных документов к архивному хранению и уничтожению.	**Содержание**		**12**	
	1.	Экспертиза ценности конфиденциальных документов.	2	2
	2.	Подготовка конфиденциальных документов и дел к архивному хранению.	2	2
	3.	Хранение архивных документов	2	
	4.	Подготовка конфиденциальных документов и дел к уничтожению.	2	
	5.	Уничтожение документов		
	6.	Архивное хранение носителей информации		
	Практические занятия		**4**	
	1.	Экспертиза ценности конфиденциальных документов.		
	2.	Подготовка конфиденциальных документов дел ля архивного хранения и уничтожения.		
Тема 7. Режим конфиденциальности документированной информации.	**Содержание**		**6**	
	1	Формы обмена конфиденциальной информацией	2	
	2	Режим обмена конфиденциальной документированной информацией.	2	2
	3	Учет и регистрация носителей конфиденциальной информации.		2
	Практические занятия		**2**	
	1.	Обмен конфиденциальной документированной информацией.		

	2.	Проверка наличия носителей конфиденциальной информации.		
Зачетная работа 8 семестре			**2**	
Самостоятельная работа при изучении раздела 3.			**47**	
Систематическая проработка конспектов занятий, учебной и специальной литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем). Подготовка к практическим работам с использованием методических рекомендаций преподавателя, оформление практических работ, отчетов и подготовка к их защите.				
Тематика внеаудиторной самостоятельной работы Изучение нормативных документов. Выполнение рефераты по темам. Оформление пакета документов, связанных с электронным документооборотом.				
Производственная практика			**72**	
Всего:			**842**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Требования к материально-техническому обеспечению

Реализация профессионального модуля требует наличия:

- учебного кабинета
- лабораторий:

Технические средства обучения:

Занятия проводятся в учебной аудитории и компьютерном классе, оснащенных необходимым учебным, методическим, информационным, программным обеспечением.

Оборудование лаборатории и рабочих мест лаборатории:

Занятия проводятся в учебной аудитории и компьютерном классе, оснащенных необходимым учебным, методическим, информационным, программным обеспечением.

3.2. Информационное обеспечение реализации профессионального модуля

Основные источники:

1. Кубашева, Е.С. Информатика и вычислительная техника. Информационная безопасность автоматизированных систем: Е.С. Кубашева, И.А. Малашкевич, Е.Н. Чекулаева; Поволжский государственный технологический университет. – Йошкар-Ола: ПГТУ, 2019. – 66 с.: (http://biblioclub.ru/index.php?page=book&id=562246)
2. Информационная безопасность: учеб./ под ред. В.П. Мельникова. - М.: Кнорус, 2018. –Рек. ФИРО
3. Вычислительная техника: Уч.пос. / Т.Л. Партыка – 3-е изд. - М.: Форум, НИЦ ИНФРА-М, 2018. – 445 с. - (Профессиональное образование)

Дополнительные источники:

1. Родичев Юрий Андреевич. Нормативная база и стандарты в области информационной безопасности. М.: Питер. Серия: учебник для вузов. 2017 г. -256 с.
2. С.А. Нестеров. Основы информационной безопасности. М.: Лань. Серия: учебник для вузов. Специальная литература. 2017 г. -324 с.
3. В.В. Бондарь. Введение в информационную безопасность автоматизированных систем. М.: МГТУ им. Н. Э. Баумана. 2017 г. -252 с.
4. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В.Ф. Шаньгин. – М.: ИД «ФОРУМ»: ИНФРА-М, 2017. – 416 с.: ил. - (Профессиональное образование). – Рек. МО

Перечень интернет-ресурсов, других источников:

1. Системы безопасноти предприятия. https://studopedia.ru/18_46205_sistema-bezopasnosti-predpriyatiya.html
2. Система безопасности. http://datasolution.ru/sistema-bezopasnosti-predpriyatiya-2
3. Обеспечение организации системы безопасности предприятия. https://itforever.jimdo.com

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Контроль и оценка результатов освоения профессионального модуля осуществляется педагогическим работником в процессе проведения практических и лабораторных занятий, контрольных работ, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Контролируемые разделы / темы	**Код и этапы формирования компетенции (или ее части)**	**Оценочные средства**	
		текущий контроль	**промежуточная аттестация**
МДК.1.1 Обеспечение организации систем безопасности предприятия			
Раздел 1	**ОК 1- ОК 12**	**Практические работы**	**Экзамен**
Тема 1.1	**ОК 1- ОК 12**	**Практические работы**	
Тема 1.2	**ОК 1- ОК 12**	**Практические работы**	
Тема 1.3	**ОК 1- ОК 12**	**Практические работы**	
Раздел 2	**ОК 1- ОК 12**	**Практические работы**	**Экзамен**
Тема 2.1	**ОК 1- ОК 12**	**Практические работы**	
Тема 2.2	**ОК 1- ОК 12**	**Практические работы**	
Раздел 3	**ОК 1- ОК 12**	**Практические работы**	**Экзамен**
Тема 3.1	**ОК 1- ОК 12**	**Практические работы**	
Тема 3.2	**ОК 1- ОК 12**	**Практические работы**	
Тема 3.3	**ОК 1- ОК 12**	**Практические работы**	
Раздел 4	**ОК 1- ОК 12**	**Практические работы**	**Экзамен**
Тема 4.1	**ОК 1- ОК 12**	**Практические работы**	
Тема 4.2	**ОК 1- ОК 12**	**Практические работы**	
Тема 4.3	**ОК 1- ОК 12**	**Практические работы**	
Тема 4.4	**ОК 1- ОК 12**	**Практические работы**	
МДК.1.2 Организация работ подразделений защиты информации			
Раздел 1	**ОК 1- ОК 12**	**Практические работы**	**Экзамен**
Тема 1.1	**ОК 1- ОК 12**	**Практические работы**	
Тема 1.2	**ОК 1- ОК 12**	**Практические работы**	

Раздел 2	**ОК 1- ОК 12**	**Практические работы**	**Экзамен**
Тема 2.1	**ОК 1- ОК 12**	**Практические работы**	
Тема 2.2	**ОК 1- ОК 12**	**Практические работы**	
Раздел 3	**ОК 1- ОК 12**	**Практические работы**	**Экзамен**
Тема 3.1	**ОК 1- ОК 12**	**Практические работы**	
Тема 3.2	**ОК 1- ОК 12**	**Практические работы**	
Тема 3.3	**ОК 1- ОК 12**	**Практические работы**	
Учебная практика			
Производственная практика			

Методические материалы, определяющие процедуры оценивания результатов освоения профессионального модуля

МДК.1.1 Обеспечение организации систем безопасности предприятия Оценочные средства для текущего контроля успеваемости

Проектная работа

Тема: Модель угроз безопасности информационной системы на базе колледжа “ЯКИТ”

Цель: Научится работать с нормативными ссылками, описывать объект организации, выявлять возможных нарушителей организации

Задачи:

1. Общие положения о организации
2. Нормативные ссылки
3. Описание информационной системы и особенностей ее функционирования
4. Возможные нарушители

Вывод

МДК.1.2 Организация работ подразделений защиты информации

Проектная работа

Автоматизирование системы на базе колледжа “ЯКИТ”

1. Собрать данные о колледже
2. Собрать данные о программах и сделать анализ

Описать программы

Перечислить плюсы и минусы программ

Сделать вывод

1. Переход с бумажного на автоматизированные системы (3 примера)

Какие программы будут использоваться

Плюсы и минусы перехода на автоматизированную систему

Вывод

1. Угрозы автоматизированных систем
1. Способы защиты автоматизированных систем

Оценочные средства для промежуточной аттестации

Кол-во баллов	Оценка	Критерии оценки
91 - 100	отлично	студент должен: продемонстрировать глубокое и прочное усвоение знаний материала; исчерпывающе, последовательно, грамотно и логически стройно изложить теоретический материал и выполнить практический материал; правильно формулировать определения; продемонстрировать умения самостоятельной работы с программой; уметь сделать выводы по излагаемому материалу
71 - 90	хорошо	студент должен: продемонстрировать достаточно полное знание материала; продемонстрировать знание основных теоретических понятий и выполнить практический материал; достаточно последовательно, грамотно и логически стройно излагать материал; продемонстрировать умение ориентироваться в литературе; уметь сделать достаточно обоснованные выводы по излагаемому материалу
51 - 70	удовлетворительно	студент должен: продемонстрировать общее знание изучаемого материала; знать основную рекомендуемую программой дисциплины учебную литературу; уметь строить ответ в соответствии со структурой излагаемого вопроса; показать общее владение понятийным аппаратом дисциплины.
Менее 51	неудовлетворительно	ставится в случае: незнания значительной части программного материала; не владения понятийным аппаратного модуля; существенных ошибок при изложении учебного материала; неумения строить ответ в соответствии со структурой излагаемого вопроса; неумения делать выводы по излагаемому материалу.