Министерство образования и науки РС (Я)
ГБПОУ РС (Я) «Ленский технологический техникум»
филиал «Пеледуйский»

Утверждено на МС
протокол № 44 а от « 6 » сентября 2022 г

Рабочая программа дисциплины

ОП 7. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Основной профессиональной образовательной программы подготовки квалифицированных рабочих, служащих по профессии
09.01.03 «Мастер по обработке цифровой информации»

Форма подготовки очная

п. Пеледуй, 2022 год

Аннотация программы

Рабочая программа учебной дисциплины ОП 7. «Информационная безопасность» разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по профессии 09.01.03 «Мастер по обработке цифровой информации» из вариативной части.

Организация-разработчик:

Государственное бюджетное профессиональное образовательное учреждение
Республики Саха (Якутия)«Ленский технологический техникум»
филиал «Пеледуйский»

Разработчики:

1.Дубинин Кирилл Владимрович, преподаватель 1 категории

Рассмотрено и рекомендовано
Методическим советом
Протокол № 44 а « 06 » сентября 2022 г.

Председатель _____ /Вавилова Е.Ю. /

СОДЕРЖАНИЕ

1. Паспорт рабочей программы учебной дисциплины «Информационная безопасность»

1.1. Область применения программы

Рабочая программа учебной дисциплины является частью основной профессиональной образовательной программы подготовки квалифицированных рабочих, служащих в соответствии с ФГОС 09.01.03 «Мастер по обработке цифровой информации»

Рабочая программа учебной дисциплины может быть использована:

— как дополнительные модули обучения в интеграции с предметами «Информатика» и (или) «ОБЖ»

— в рамках отдельного учебного курса «Информационная безопасность» для внеурочной деятельности по выбору из объема часов, формируемых самостоятельно образовательной организацией;

— в рамках часов, предусмотренных по программе воспитания (социализации) в образовательной организации для разных уровней общего образования

1.2. Место учебной дисциплины в структуре основной профессиональной образовательной программы/программы подготовки квалифицированных рабочих, служащих: учебная дисциплина входит в профессиональный цикл как общепрофессиональная дисциплина

1.3. Цели и задачи учебной дисциплины – требования к результатам освоения учебной дисциплины.

Обучающийся, освоивший дисциплину, должен обладать следующими знаниями:

- сущность и понятие информационной безопасности, характеристику ее составляющих;
- место информационной безопасности в системе национальной безопасности страны;
- виды, источники и носители защищаемой информации;
- источники угроз безопасности информации и меры по их предотвращению;
- факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
- жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
- современные средства и способы обеспечения информационной безопасности;
- основные методики анализа угроз и рисков информационной безопасности.

Обучающийся, освоивший дисциплину, должен обладать следующими умениями:

- классифицировать защищаемуюинформацию по видам тайны истепеням секретности;
- классифицировать основные угрозы безопасности информации.

1.4. Рекомендуемое количество часов на освоение программы учебной дисциплины:

максимальной учебной нагрузки обучающегося 68 часов, в том числе:

- обязательной аудиторной учебной нагрузки обучающегося 46 часа;

- самостоятельной работы обучающегося 22часов.

2. Структура и содержание рабочей программы учебной дисциплины

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем

	часов
Максимальная учебная нагрузка (всего)	*68*
Обязательная аудиторная учебная нагрузка (всего)	*46*
в том числе:	
лабораторные работы	-
практические занятия	*38*
контрольные работы	-
курсовая работа (проект) (*если предусмотрено)*	-
Самостоятельная работа обучающегося (всего)	*22*
Итоговая аттестация в форме дифференцированного зачета	

3.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Объем часов	Уровень освоения
Раздел 1.Основные составляющиеинформационной безопасности			
Тема 1.1 Основные понятия информационной безопасности.	**Содержание учебного материала**	**2**	
	Классификация угроз. Классификация средств защиты информации. Методы и средства организационно-правовой защиты информации. Методы и средства инженерно-технической защиты	*1*	2
	Программные и программно-аппаратные методы и средства обеспечения информационной безопасности	*1*	
	Самостоятельная работа обучающихся	**6**	
	Изучение дополнительной литературы и других источников	*6*	3
Раздел 2. Средства защиты информации			
Тема 2.1 Криптографические способы защиты информации	**Содержание учебного материала**	**2**	
	Введение в основы современных шифров с симметричнымключом. Модульная арифметика. Сравнения и матрицы. Традиционные шифры с симметричным ключом. Алгебраическиеструктуры. Поля. Усовершенствованный стандарт шифрования(AES — AdvancedEncryptionStandard). Простыечисла. Квадратичное сравнение. Криптографическая система RSA. Криптосистемы. Простые криптосистемы.	*1*	2
	Шифрованиеметодомзамены(подстановки). Одноалфавитнаяподстановка. Многоалфавитная одноконтурная обыкновенная подстановка. Таблицы Вижинера. Многоалфавитная одноконтурная монофоническая подстановка. Многоалфавитная многоконтурная подстановка. Шифрование методом перестановки. Простая перестановка. Перестановка, усложненная по таблице. Перестановка, усложненная по маршрутам. Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования. Стандартышифрования. Стандарт шифрования данных DataEncryptionStandard. Режимы работы алгоритма DES. Алгоритм шифрования данных IDEA. Общая схема алгоритма IDEA	*1*	
	Самостоятельная работа обучающихся	**6**	
	Изучение дополнительной литературы и других источников	*6*	3
Тема 2.2 Антивирусная защита	**Содержание учебного материала**	**2**	
	Общие понятия антивирусной защиты. Уязвимости. Классификация вредоносных программ. Признаки присутствия накомпьютере вредоносных программ.	*1*	2

	Методы защиты от вредоносных программ.		
	Основы работы антивирусных программ. Сигнатурный и эвристический анализ. Классификация антивирусов. Режимы работы антивирусов. Антивирусные комплексы	*1*	
	Практические занятия	**30**	
	Использование встроенных средств защиты системы	*2*	3
	Установка бесплатных антивирусных программ на примере AVG, Avira, Avast.	*2*	
	Настройка и обновление бесплатных антивирусных программ на примере AVG, Avira, Avast.	*2*	
	Установка средств защиты от лаборатории «Касперский» и доктор ВЭБ.	*4*	
	Настройка и обновление средств защиты от лаборатории «Касперский» и доктор ВЭБ	*2*	
	Проверка компьютера на наличие угроз	*4*	
	Проверка носителей на наличие угроз	*4*	
	Использование специальных антивирусных утилит, исправляющих последствия вирусной атаки	*6*	
	Борьба с рекламными и шпионскими программами	*2*	
	Настройка межсетевого экрана	*2*	
	Самостоятельная работа обучающихся	**4**	
	Изучение дополнительной литературы и других источников	*2*	3
	Подготовка к практическим работам	*2*	
Раздел 3. Сетевая безопасность			
Тема 3.1 Защита информации в компьютерных сетях	**Содержание учебного материала**	**2**	
	Уровни антивирусной защиты.Уровень защиты рабочих станций и сетевых серверов. Уровеньзащиты почты. Уровень защиты шлюзов. Централизованноеуправление антивирусной защитой. Логическая сеть. Схемасбора статистики в системе антивирусной защиты. Управление ключами шифрования и безопасность сети. Целостность сообщения и установление подлинности сообщения. Криптографические хэш-функции. Цифровая подпись. Установлениеподлинности объекта. Управление ключами.	*1*	2
	Безопасность на прикладном уровне. Безопасность на транспортном уровне. Безопасность на сетевом уровне.	*1*	
	Практические занятия	**8**	
	Парольный доступ и парольная аутентификация	*4*	3
	Создание цифровой подписи	*4*	
	Самостоятельная работа обучающихся	**6**	
	Изучение дополнительной литературы и других источников	*2*	3
	Подготовка к практическим работам	*4*	
	Всего:	**68**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:
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 учебной дисциплины

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины предполагает наличие учебного кабинета.

Оборудование учебного кабинета:

- рабочее место преподавателя;
- рабочие места по количеству обучающихся;
- наглядные пособия (таблицы, схемы и т.д.).

Технические средства обучения:

- компьютер по количеству обучающихся;
- видеопроектор;
- интерактивная доска

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Клейменов С.А., Мельников В.П. Информационная безопасность. Учебное пособие для студентов учреждений среднего профессионального образования. Гриф МО РФ. 7-е изд. - М.: Издательство: Академия, 2012. – 336 с.

Дополнительные источники:

1. Попов В.Б. Основы информационных и телекоммуникационных технологий. Основы информационной безопасности: Учебное пособие – М.: Финансы и статистика, 2005. – 176 с.
2. С. П. Расторгуев Основы информационной безопасности – М.: Академия, 2007. – 192 с.
3. Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов Основы информационной безопасности – М.: Горячая Линия – Телеком, 2006. – 544 с.

4. Цирлов В.Л. Основы информационной безопасности: краткий курс/Профессиональное образование. – М.: Феникс, 2008. – 400 с.

Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине:

1. Лапонина О.Р. Криптографические основы безопасности – [Электронный ресурс] – URL: http://www.intuit.ru/
2. Фороузан Б.А. Математика криптографии и теория шифрования. Пер. А.Н. Берлин. – [Электронный ресурс] – URL http://www.intuit.ru/
3. Конеев И.Р. Информационная безопасность предприятия. [Текст]./ И.Р.Конеев, А.В.Беляев. - СПб.: БХВ-Петербург, 2003

Интернет-ресурсы:

1. http://fcior.edu.ru/ - Федеральный центр информационно- образовательных ресурсов
2. http://www.edu.ru/ - Федеральные образовательные ресурсы
3. https://www.kaspersky.ru/ – Web-сайт разработчиков антивируса «Касперский»
4. https://www.drweb.ru/ – Web-сайт разработчиков антивируса «доктор ВЭБ»
5. https://www.avg.com/ - Web-сайт разработчиков антивируса «AVG»
6. https://www.avira.com/- Web-сайт разработчиков антивируса «Avira»
7. https://www.avast.ru/– Web-сайт разработчиков антивируса «Avast»

5. Контроль и оценка результатов освоения учебной дисциплины

Основной целью оценки освоения учебной дисциплины является оценка освоенных умений и усвоенных знаний.

Оценка качества освоения учебной дисциплины включает текущий контроль знаний, промежуточную и итоговую аттестацию обучающихся.

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

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Знания: - сущность и понятие информационной безопасности, характеристику ее составляющих; - место информационной безопасности в системе национальной безопасности страны; - виды, источники и носители защищаемой информации; - источники угроз безопасности информации и меры по их предотвращению; - факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; - жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; - современные средства и способы обеспечения информационной безопасности; - основные методики анализа угроз и рисков информационной безопасности.	Устный опрос Экспертная оценкарезультатов деятельностиобучающегося при выполнении изащите результатов практическихзанятий.
Умения: - классифицировать защищаемуюинформацию по видам тайны истепеням секретности; - классифицировать основные угрозы безопасности информации.	Устный опрос Экспертная оценкарезультатов деятельностиобучающегося при выполнении изащите результатов практическихзанятий.

Итоговой аттестацией по дисциплине является дифференцированный зачет

Разработчики:

- Преподаватель Дубинин К.В./_____/