

МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Якутская государственная сельскохозяйственная академия»
Колледж технологий и управления
Цикловая комиссия гуманитарных и естественных дисциплин

Регистрационный
номер 24-22/15

УТВЕРЖДАЮ

Проректор по учебной и
воспитательной работе



Черкашина А.Г.

06 20 19 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Дисциплина	ОП.13 Информационная безопасность
Специальность	09.02.07 Информационные системы и программирование
Квалификация	Программист
Уровень ППССЗ	базовая
Срок освоения ППССЗ	3 года 10 месяцев
Форма обучения	очная
Общая трудоемкость	32 ч

Якутск 2019

Рабочая программа учебной дисциплины разработана в соответствии с:
- Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.07 Информационные системы и программирование, утвержденный приказом Министерства образования и науки Российской Федерации от 09.12.2016 г. № 1547.
- Учебным планом специальности 09.02.07 Информационные системы и программирование одобрен Ученым советом ФГБОУ ВО Якутская ГСХА от 04.04.2019 г., протокол №23/2.

Разработчик(и) РПД Вилтракис Геннадий Владимирович - преподаватель

Цикловая комиссия теплоснабжения _____ /Машиев Ч.Г./

Протокол заседания ЦК № 10 от «18» 06 2019 г.

Директор КТиУ _____ /Яковлева Н.М./
подпись фамилия, имя, отчество
«25» 06 2019 г.

Методист _____ /Местникова М.А./
подпись фамилия, имя, отчество

Протокол заседания № 10 от «24» 06 2019 г.

Председатель УМС ЯГСХА _____ /Сивцев Н.А./
подпись фамилия, имя, отчество

Протокол заседания УМС № 4 от «25» 06 2019 г.

СОДЕРЖАНИЕ

№	Наименование раздела	Стр.
1	Общая характеристика рабочей программы учебной дисциплины	4
2	Структура и содержание учебной дисциплины	6
3	Условия реализации учебной дисциплины	9
4	Контроль и оценка результатов освоения учебной дисциплины	11

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.13 Информационная безопасность

1.1. Область применения программы

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена в соответствии с ФГОС по специальности (специальностям) СПО 09.02.07 Информационные системы и программирование.

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

Учебная дисциплина «Информационная безопасность» относится к общепрофессиональному циклу.

Освоение дисциплины способствует формированию компетенций:

ОК 01. Выбирать способы решения задач в профессиональной деятельности, применительно к различным контекстам;

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности;

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами;

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста;

ОК 09. Использовать информационные технологии профессиональной деятельности;

ОК 10. Пользоваться профессиональной на государственном и иностранном языке.

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

Программа ориентирована на достижение следующих целей:

•усвоение знаний по нормативно-правовым основам организации информационной безопасности, изучение стандартов и руководящих документов по защите информационных систем;

•ознакомление с основными угрозами информационной безопасности;

•правилами их выявления, анализа и определение требований к различным уровням обеспечения информационной безопасности;

•формирование научного мировоззрения, навыков индивидуальной самостоятельной работы с учебным материалом.

Содержание каждой темы включает теоретический и практико- ориентированный материал, реализуемый в форме лабораторной работы с использованием средств ИКТ.

В результате освоения учебной дисциплины обучающийся должен уметь:

- У.1 классифицировать компьютерные вирусы.

- У.2 определять вирусоподобные программы по характерным признакам

- У.3 классифицировать антивирусные программы

- У.4 использовать механизмы идентификации и аутентификации для защиты информационных систем.

В результате освоения учебной дисциплины обучающийся должен знать:

- 3.1 характерные черты компьютерных вирусов;

- 3.2 проблемы при определении компьютерного вируса.

- 3.3 классы компьютерных вирусов;

- 3.4 характеристики различных компьютерных вирусов.

- 3.5 принципы защиты распределенных вычислительных сетей

1.4. Рекомендуемое количество часов на освоение программы учебной дисциплины:

Максимальной учебной нагрузки обучающегося 32 часа, в том числе:

- обязательной аудиторной учебной нагрузки обучающегося 32 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	32
Обязательная аудиторная учебная нагрузка (всего)	32
в том числе:	
лекции	16
практические занятия	16
<i>Итоговая аттестация в форме зачета в пятом семестре</i>	

2.2. Тематический план и содержание учебной дисциплины Информационная безопасность

<i>Наименование разделов и тем</i>	<i>Содержание учебного материала и формы организации деятельности обучающихся</i>	<i>Объем в часах</i>	<i>Уровень освоения</i>
	Раздел 1. Информационная безопасность и уровни ее обеспечения	6	
Тема 1. Понятие "информационная безопасность"	Содержание учебного материала	6	1,2
	.Понятие "информационная безопасность". Задачи информационной безопасности, уровни формирования режима информационной безопасности. Нормативно-правовые основы информационной безопасности. Стандарты информационной безопасности в РФ. Классификация угроз "информационной безопасности".		
	В том числе практических занятий	2	1,2,3
	Раздел 2. Компьютерные вирусы и защита от них.	8	
Тема 2. Вирусы как угроза информационной безопасности	Содержание учебного материала	8	1,2
	Вирусы как угроза информационной безопасности. Классификация компьютерных вирусов. Характеристика "вирусоподобных" программ. Антивирусные программы. Профилактика компьютерных вирусов. Обнаружение неизвестного вируса.		
	В том числе практических занятий	6	1,2,3
	Раздел 3. Информационная безопасность вычислительных сетей		

Тема 3.	Содержание учебного материала	8	
Особенности обеспечения информационно-й безопасности в компьютерных сетях.	Особенности обеспечения информационной безопасности в компьютерных сетях. Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO. Адресация в глобальных сетях. Классификация удаленных угроз в вычислительных сетях. Типовые удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях. Принципы защиты распределенных вычислительных сетей	8	1,2
	<i>В том числе практических занятий</i>	4	1,2,3
	Раздел 4. Механизмы обеспечения "информационной безопасности"	8	
Тема 4.	Содержание учебного материала	8	
Идентификация и аутентификация.	Тема 4. Идентификация и аутентификация. Криптография и шифрование. Методы разграничение доступа. Регистрация и аудит. Межсетевое экранирование. Технология виртуальных частных сетей (VPN) составляющие технологии виртуальных частных сетей.		1,2
	<i>В том числе практических занятий</i>	4	1,2,3
<i>Примерный перечень практических работ:</i>			
1. распределять задачи информационной безопасности по уровням ее обеспечения			
2. определять политику безопасности организации, Конституция Российской Федерации, доктрина информационной безопасности Российской Федерации, федеральные законы в области информации и информационной безопасности, указы президента РФ и постановления правительства РФ в области информации и информационной безопасности, правовые режимы защиты информации.			
3. выявлять и классифицировать угрозы информационной безопасности			
4. проводить профилактику компьютерных вирусов.			
5. проверить систему на наличие макровируса			
6. использовать модель OSI/ISO для описания процесса передачи данных между узлами компьютерной сети.			
7. преобразовывать двоичный IP-адрес в десятичный, определять тип сети по IP-адресу.			
8. классифицировать типовые удаленные атаки по совокупности признаков.			
9. использовать электронную цифровую подпись для проверки целостности данных.			
10. использовать механизмы регистрации и аудита для анализа защищенности системы.			
<i>Всего:</i>		32	

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечения

№ п\п	Наименование дисциплины (модуля), практик в соответствии с учебным планом	Наименование специальных* помещений и помещений для самостоятельной работы	Оснащенность специальных помещений и помещений для самостоятельной работы
1	ОП.13 Информационная безопасность	Лаборатория информационных ресурсов 677007, Республика Саха (Якутия), г. Якутск, ш. Сергеляхское, 3 км, д.3, 4 этаж, №14	Оборудование: Автоматизированные рабочие места на 15 обучающихся (обучающихся с конфигурацией: Core i5 дискретная видеокарта, 8GB ОЗУ, один или два монитора 23", 24"ViewsonicVA2407h, мышь, клавиатура; Автоматизированное рабочее место преподавателя (Rusco Core-i5-7100/2*4Gb/500Gb/Win10Pro/Office, монитор (22"Benq GL2250) – 1; Учебная мебель: компьютерный стол (СК № 20164 (КР - груша, Д - 024)) – 22 шт.; стул подъемно-поворотный – 16 шт Офисный мольберт (флипчарт); Проектор и экран; Маркерная доска; Принтер А3, цветной; МФУ формата А4; Программное обеспечение общего и профессионального назначения

3.2. Информационное обеспечение обучения

Перечень учебных изданий, интернет-ресурсов, дополнительной литературы

Основные источники:

№	Наименование	Авторы	Год и место издания	Используется при изучении тем	Семестр
1	2	3	4	5	6
1	Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / — 342 с Режим доступа: https://www.biblio-online.ru/viewer/osnovy-informacionnoy-bezopasnosti-nadezhnost-i-bezopasnost-programmnogo-obespecheniya-456792#page/1	О. В. Казарин, И. Б. Шубинский.	Москва: Издательство Юрайт, 2020	1-4	5

Перечень электронных ресурсов:

№	Наименование
Э1	www.fcior.edu.ru (Федеральный центр информационно-образовательных ресурсов — ФЦИОР).
Э2	www.school-collection.edu.ru (Единая коллекция цифровых образовательных ресурсов).
Э3	www.intuit.ru/studies/courses (Открытые интернет-курсы «Интуит» по курсу «Информатика»)
Э4	www.lms.iite.unesco.org (Открытые электронные курсы «ИИТО ЮНЕСКО» по информационным технологиям).
Э5	http://ru.iite.unesco.org/publications (Открытая электронная библиотека «ИИТО ЮНЕСКО» по ИКТ в образовании).
Э6	www.megabook.ru (Мегаэнциклопедия Кирилла и Мефодия, разделы «Наука / Математика. Кибернетика» и «Техника / Компьютеры и Интернет»).
Э7	www.ict.edu.ru (портал «Информационно-коммуникационные технологии в образовании»).
Э8	www.digital-edu.ru (Справочник образовательных ресурсов «Портал цифрового образования»)
Э9	www.window.edu.ru (Единое окно доступа к образовательным ресурсам Российской Федерации)
Э10	www.freeschool.altlinux.ru (портал Свободного программного обеспечения)
Э11	www.hear.altlinux.org/issues/textbooks (учебники и пособия по Linux)
Э12	www.books.altlinux.ru/altlibrary/openoffice (электронная книга «OpenOffice.org: Теория и практика»)
Э1	Учебники по программированию http://programm.ws/index.php

Перечень информационных справочных систем:

№	Наименование
1	Информационно-правовая система Гарант

3.3. Условия реализации учебной дисциплины для студентов-инвалидов и лиц с ограниченными возможностями здоровья

3.3.1. Образовательные технологии.

С целью оказания помощи в обучении студентов-инвалидов и лиц с ОВЗ применяются образовательные технологии с использованием универсальных, специальных информационных и коммуникационных средств.

Для основных видов учебной работы применяются:

Контактная работа:

- лекции – проблемная лекция, лекция-дискуссия, лекция-диалог, лекция-консультация, лекция с применением дистанционных технологий и привлечением возможностей Интернета;
- практические (семинарские) занятия - практические задания;
- групповые консультации – опрос, работа с лекционным и дополнительным материалом;
- индивидуальная работа с преподавателем - индивидуальная консультация, работа с лекционным и дополнительным материалом, беседа, морально-эмоциональная поддержка и стимулирование, дистанционные технологии.

Формы самостоятельной работы устанавливаются с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге или на компьютере).

В качестве самостоятельной подготовки в обучении используется - система дистанционного обучения Moodle (sdo.ysaa.ru).

Самостоятельная работа:

- работа с книгой и другими источниками информации, план-конспекты;
- творческие самостоятельные работы;
- дистанционные технологии.

При необходимости обучающимся предоставляется дополнительное время для консультаций и выполнения заданий.

3.3.2. Специальное материально-техническое и учебно-методическое обеспечение.

При обучении по дисциплине используется система, поддерживающая дистанционное образование - «Moodle» (sdo.ysaa.ru), ориентированная на организацию дистанционных курсов, а также на организацию взаимодействия между преподавателем и обучающимися посредством интерактивных обучающих элементов курса.

Для обучающихся лиц с нарушением зрения предоставляются:

- видеувеличитель-монокуляр для просмотра Levenhuk Wise 8x25;
- электронный ручной видеувеличитель видео оптик “wu-tv”;
- возможно также использование собственных увеличивающих устройств;
- версия сайта академии <http://www.ysaa.ru/> для слабовидящих.

Для обучающихся лиц с нарушением слуха предоставляются:

- аудитории со звукоусиливающей аппаратурой (колонки, микрофон);
- компьютерная техника в оборудованных классах;
- учебные аудитории с мультимедийной системой с проектором;
- аудитории с интерактивными досками в аудиториях;
- учебные пособия, методические указания в форме электронного документа

Для обучающихся лиц с нарушениями опорно-двигательного аппарата предоставляются:

- система дистанционного обучения Moodle (sdo.ysaa.ru);
- учебные пособия, методические указания в форме электронного документа/

3.3.3. Контроль и оценка результатов освоения учебной дисциплины.

Контроль результатов обучения осуществляется в процессе проведения практических занятий, выполнения индивидуальных самостоятельных работ.

Формы и сроки проведения рубежного контроля определяются с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.), и может проводиться в несколько этапов.

При необходимости, предоставляется дополнительное время для подготовки ответов на зачете, аттестация проводится в несколько этапов (по частям), во время аттестации может присутствовать ассистент, аттестация прерывается для приема пищи, лекарств, во время аттестации используются специальные технические средства.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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.

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения
Итоговый контроль:	Зачет
Уметь	
У.1 классифицировать компьютерные вирусы	<ul style="list-style-type: none"> •Тестирование. •Контрольная работа •Самостоятельная работа. •Наблюдение за выполнением практического задания. (деятельностью студента) •Оценка выполнения практического задания(работы)
У.2 определять вирусоподобные программы по характерным признакам	
У.3 классифицировать антивирусные программы	
У.4 использовать механизмы идентификации и аутентификации для защиты информационных систем	
Знать	
З.1 характерные черты компьютерных вирусов	
З.2 проблемы при определении компьютерного вируса	
З.3 классы компьютерных вирусов	
З.4 характеристику различных компьютерных вирусов	
З.5 принципы защиты распределенных вычислительных сетей	

**Лист изменений и дополнений рабочей программы
по учебной дисциплине ОП. 13 Информационная безопасность**

В соответствии с актуальным перечнем учебной литературы по договору с ЭБС «Юрайт» вносятся следующие изменения в рабочую программу учебной дисциплины

Раздел 3.2

ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

1. Основы информационной безопасности: надежность и безопасность программного обеспечения/ Казарин О.В., Шубинский И.Б. учебное пособие для СПО — Москва : Издательство Юрайт, 2020. — 342 с

Рабочая программа учебной дисциплины (модуля) пересмотрена и одобрена:

Председатель ЦК гуманитарных и
естественных дисциплин _____ /

Н.К.Лотова

Протокол от «05» февраля 2020 г., № 7.

Председатель МК КТиУ _____

Ю.В. Чиркова

Протокол заседания МК факультета от «07» февраля 2020 г., № 6.