ЧАСТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САЯНСКИЙ ТЕХНИКУМ СТЭМИ»

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.13 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

по специальности

09.02.07 Информационные системы и программирование

Саяногорск,
2023 г.

Рассмотрена
на заседании педагогического совета
Протокол № ___1_____
от «_28_» ___08____ 2023 г.

Утверждено директором ЧОУ ПО СТЭМИ
М.Н. Соболев

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 6B8E3B4A05DCC2E2D616152D0BD84BE8
Владелец: Соболев Максим Николаевич
Действителен: с 09.11.2023 до 01.02.2025

Рабочая программа учебной дисциплины ОП.13 Информационная безопасность разработана на основе Федерального государственного образовательного стандарта по специальности 09.02.07 Информационные системы и программирование, утверждённого Приказом Минпросвещения России от 09.12.2016 N 1547 (Зарегистрировано в Минюсте России 26.12.2016 N 44936).

Организация разработчик: ЧОУ ПО «Саянский техникум СТЭМИ»

Составитель: Учебно-методический отдел ЧОУ ПО СТЭМИ.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
ОП.13 Информационная безопасность

1.1. Место дисциплины в структуре основной образовательной программы:

Учебная дисциплина ОП.13 Информационная безопасность является вариативной частью общепрофессионального цикла основной образовательной программы в соответствии с ФГОС СПО по специальности 09.02.07 Информационные системы и программирование.

Особое значение дисциплина имеет при формировании и развитии общих и профессиональных компетенций:

Общие компетенции (ОК):

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

ОК 02 Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;

ОК 04. Эффективно взаимодействовать и работать в коллективе и команде;

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

ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках.

Профессиональные компетенции (ПК):

ПК 5.3. Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием.

ПК 6.4. Оценивать качество и надежность функционирования информационной системы в соответствии с критериями технического задания.

ПК 7.5. Проводить аудит систем безопасности баз данных и серверов с использованием регламентов по защите информации.

1.2. Цель и планируемые результаты освоения дисциплины:

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания

Код ПК, ОК	Умения	Знания
ОК 01, ОК 02, ОК 04, ОК 05, ОК 09 ПК 5.3, ПК 6.4 ПК 7.5	использовать методы защиты программного обеспечения компьютерных систем; − анализировать риски и характеристики качества программного обеспечения; − выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами; − применять стандартные методы для защиты объектов базы данных; − выполнять стандартные процедуры резервного копирования и мониторинга выполнения этой процедуры; − выполнять процедуру восстановления базы данных и вести мониторинг выполнения этой процедуры; − выполнять установку и настройку программного обеспечения для обеспечения работы пользователя с базой данных; − обеспечивать информационную безопасность на уровне базы данных.	− технологии передачи и обмена данными в компьютерных сетях; − алгоритм проведения процедуры резервного копирования; − алгоритм проведения процедуры восстановления базы данных; − методы организации целостности данных; − способы контроля доступа к данным и управления привилегиями; − основы разработки приложений баз данных; − основные методы и средства защиты данных в базе данных.

Личностные результаты реализации программы воспитания (ЛР):

ЛР 3 Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих.

ЛР 4 Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа».

ЛР 13 Демонстрирующий умение эффективно взаимодействовать в команде, вести диалог, в том

числе с использованием средств коммуникации

ЛР 14 Демонстрирующий навыки анализа и интерпретации информации из различных источников с учетом нормативно-правовых норм

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем в часах
Объем образовательной программы учебной дисциплины	**76**
в т. ч.:	
теоретическое обучение	38
лабораторные работы	-
практические занятия	20
курсовая работа (проект)	-
Самостоятельная работа	10
Консультация	2
Промежуточная аттестация: дифференцированный зачёт	6

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций, формированию которых способствует элемент программы
Раздел 1. Информационная безопасность и уровни ее обеспечения		**10**	
Тема 1.1. Понятие и составляющие информационной безопасности	**Содержание учебного материала**	**10**	ОК 01, ОК 02, ОК 04, ОК 05, ОК 09 ПК 5.3, ПК 6.4 ПК 7.5 ЛР 3, ЛР 4, ЛР 13, ЛР 14
	1.Основные понятия безопасности: конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации.	2	
	2.Возможные угрозы информационной безопасности: классификация, источники возникновения и пути реализации. Виды угроз. Определение требований к уровню обеспечения информационной безопасности.	2	
	3.Управление рисками. Основные понятия. Процесс оценки рисков.	2	
	4.Понятие безопасности БД. Угрозы безопасности БД: общие и специфичные. Требования безопасности БД.	2	
	В том числе практических занятий и лабораторных работ		
	Практическое занятие №1 Работа с содержанием нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами	2	
Раздел 2. Стандарты информационной безопасности		**22**	
Тема 2.1. Международные стандарты информационной безопасности и стандарты информационной безопасности в РФ	**Содержание учебного материала**	**4**	
	1.Международный стандарт информационной безопасности (ISO). Система международных и национальных стандартов безопасности информации.	2	
	2.Документы по оценке защищенности автоматизированных систем в РФ Гостехкомиссия и ее роль в обеспечении информационной безопасности в РФ. Первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности.	2	
Тема 2.2. Административный уровень обеспечения	**Содержание учебного материала**	**4**	
	1.Цели, задачи и содержание административного уровня. Разработка политики информационной безопасности. Сервисы безопасности в вычислительных сетях	2	
	В том числе практических занятий и лабораторных работ		

информационной безопасности	**Практическое занятие №2** Использование средств администрирования Windows для анализа и настройки безопасности системы. Исследование угроз доступности	2	
Тема 2.3. Классификация угроз информационной безопасности	**Содержание учебного материала**	**14**	
	1.Классы угроз информационной безопасности. Каналы несанкционированного доступа к информации.	2	
	2.Механические системы защиты. Системы оповещения о попытках вторжения. Системы опознавания нарушителей.	2	
	3.Авторизация технического контроля защиты потоков информации	2	
	4. Защита информации от копирования. Защита информации от несанкционированного доступа.	2	
	В том числе практических занятий и лабораторных работ		
	Практическое занятие №3 Проверка компьютера на предмет наличия уязвимостей. Исследование угроз доступности.	2	
	Практическое занятие №4 Защита и восстановление данных на компьютере, используя систему архивации.	2	
	Практическое занятие №5 Аварийное восстановление.	2	
Раздел 3. Компьютерные вирусы и защита от них		**26**	
Тема 3.1. Вирусы как угроза информационной безопасности	**Содержание учебного материала**	**12**	
	1.Компьютерные вирусы и информационная безопасность. Характерные черты компьютерных вирусов	2	
	2.Классификация компьютерных вирусов по среде обитания. Классификация компьютерных вирусов по деструктивным возможностям.	2	
	3.Методы и технологии борьбы с компьютерными вирусами.	2	
	4.Антивирусные программы. Классификация антивирусных программ. Антивирусные программы.	2	
	В том числе практических занятий и лабораторных работ		
	Практическое занятие №6 Исследование реестра, на предмет возможных уязвимостей для вирусов	2	
	Практическое занятие №7 Использование брандмауэров. Использование антивирусных программ	2	
Тема 3.2.	**Содержание учебного материала**	**14**	

Вирусоподобные программы	1.Виды "вирусоподобных" программ. Характеристика "вирусоподобных" программ. 2.Утилиты скрытого администрирования. "Intended"-вирусы. 3.Защита информации в сетях. Сервисы безопасности. 4.Межсетевые экраны – брандмауэры. Прокси – серверы. Системы активного аудита	2 2 2 2	
	В том числе практических занятий и лабораторных работ		
	Практическое занятие №8 Настройка межсетевого экрана. Оптимизация антивирусной программы под определенную систему. **Практическое занятие №9** Использование специальных антивирусных утилит, исправляющих последствия вирусной атаки **Практическое занятие №10** Очистка системы. Настройка антивирусной программы, обновление сигнатур. Борьба с рекламными и шпионскими программами	2 2 2	
Самостоятельная работа		**10**	
Консультация		**2**	
Промежуточная аттестация: экзамен		**6**	
Всего		**76**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Для реализации программы учебной дисциплины должны быть предусмотрены следующие специальные помещения:

Лаборатория "Программного обеспечения и сопровождения компьютерных систем" оснащенная необходимым для реализации программы учебной дисциплины оборудованием:

- Автоматизированные рабочие места на 15 обучающихся;
- Автоматизированное рабочее место преподавателя;
- Проектор и экран;
- Маркерная доска;
- Программное обеспечение общего и профессионального назначения.

3.2. Информационное обеспечение реализации программы

Библиотечный фонд укомплектован печатными и электронными изданиями основной и дополнительной учебной литературы. Информационное обеспечение реализации образовательной программы осуществляется электронной библиотекой - «Электронная библиотечная система «Консультант студента», ЭР ЦОС СПО “PROF образование”, Электронная библиотечная система «Юрайт».

Основные печатные издания

1. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. – Москва: Издательство Юрайт, 2021. – 342 с. – (Профессиональное образование). – ISBN 978-5-534-10671-8. – URL: https://urait.ru/bcode/475889

Дополнительные источники

1. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. – 3-е изд., перераб. и доп. – Москва: Издательство Юрайт, 2021. – 13 161 с. – (Профессиональное образование). – ISBN 978-5-534-13948-8. – URL: https://urait.ru/bcode/475890

2. Суворова. Г. М. Информационная безопасность: учебное пособие для вузов / Г. М. Суворова. – Москва: Издательство Юрайт, 2021. – 253 с. – (Высшее образование). – ISBN 978-5-534-13960-0. – URL: https://urait.ru/bcode/467370

3. Корабельников, С. М. Преступления в сфере информационной безопасности: учебное пособие для вузов / С. М. Корабельников. – Москва: Издательство Юрайт, 2021. – 111 с. – (Высшее образование). – ISBN 978-5-534- 12769-0. – URL: https://urait.ru/bcode/476798

4. Казарин, О. В. Надежность и безопасность программного обеспечения: учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. – Москва: Издательство Юрайт, 2021. – 342 с. – (Высшее образование). – ISBN 978-5-534- 05142-1. – URL: https://urait.ru/bcode/473348

5. Гендина, Н. И. Информационная культура личности в 2 ч. Часть 1: учебное пособие для вузов / Н. И. Гендина, Е. В. Косолапова, Л. Н. Рябцева; под научной редакцией Н. И. Гендиной. – 2-е изд. – Москва: Издательство Юрайт, 2021; Кемерово: КемГИК. – 356 с. – (Высшее образование). – ISBN 978-5-534- 14328-7 (Издательство Юрайт). – ISBN 978-5-8154-0518-9 (КемГИК). – URL: https://urait.ru/bcode/477568

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	Критерии оценки	Формы и методы оценки
Знать: - основные понятия информационной безопасности; - источники возникновения информационных угроз; - модели и принципы защиты информации от несанкционированного доступа; - способы защиты информации в персональном компьютере; - методы криптографического преобразования информации; - методы антивирусной защиты информации; - состав и методы правовой защиты информации; - проблемы и направления развития системных программных средств.	«Отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко. «Хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками. «Удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки. «Неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	Компьютерное тестирование на знание терминологии по теме; Тестирование; Самостоятельная работа; Наблюдение за выполнением практического задания. (деятельностью студента); Оценка выполнения практического задания(работы); Решение задач.
Уметь: - использовать методы защиты программного обеспечения компьютерных систем; - анализировать риски и характеристики качества программного обеспечения; - выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами; - применять стандартные методы для защиты объектов базы данных; - выполнять стандартные процедуры резервного копирования и мониторинга выполнения этой процедуры; - выполнять процедуру восстановления базы данных и вести мониторинг выполнения этой процедуры;		

- выполнять установку и настройку программного обеспечения для обеспечения работы пользователя с базой данных; - обеспечивать информационную безопасность на уровне базы данных		