МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ ПЕРМСКОГО КРАЯ
государственное бюджетное профессиональное образовательное учреждение
«Пермский химико-технологический техникум»
(ГБПОУ «ПХТТ»)

УТВЕРЖДАЮ
УТВЕРЖДАЮ
Заместитель директора
_____ О.В.Князева

Одобрено на заседании ПЦК
ИТ и программирования
Протокол № 1 от 02.09.2020

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.11 Информационная безопасность
для специальности
09.02.03 Программирование в компьютерных системах

2020

Рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее - СПО) **09.02.03 Программирование в компьютерных системах.**

Организация-разработчик:
государственное бюджетное профессиональное образовательное учреждение «Пермский химико-технологический техникум» (ГБПОУ «ПХТТ»)

Разработчик:
Котельникова В.Е. - преподаватель высшей квалификационной категории, Почетный работник СПО, ГБПОУ «ПХТТ».

СОДЕРЖАНИЕ

1. **ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ** 4

2. **СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ** 6

3. **УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ** 15

4. **КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ** 18

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины ОП.11 «Информационная безопасность» является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО **09.02.03 «Программирование в компьютерных системах»** (базовый уровень).

Рабочая программа учебной дисциплины может быть использована в дополнительном профессиональном образовании в рамках реализации программ переподготовки кадров в учреждениях СПО.

1.2. Место учебной дисциплины в структуре основной профессиональной образовательной программы:

Данная дисциплина введена за счет часов вариативной части образовательной программы специальности СПО **09.02.03 Программирование в компьютерных системах** (базовый уровень).

Учебная дисциплина «Информационная безопасность» является общепрофессиональной дисциплиной в вариативной ее части, формирующей базовый уровень знаний для освоения специальных дисциплин.

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

Цель изучения дисциплины: является формирование у обучающихся понимания основ информационной безопасности, практических навыков организации работ по обеспечению информационной безопасности на предприятиях и организациях.

Главной задачей изучения теоретического курса для обучающихся является формирование представления о роли и месте знаний по дисциплине «Информационная безопасность» при освоении смежных дисциплин по выбранной специальности и в сфере профессиональной деятельности.

В результате освоения учебной дисциплины обучающийся должен уметь:

- применять правовые, организационные, технические, программные средства защиты информации;
- применять методы разграничения полномочий пользователей и управления доступом к ресурсам в защищенных операционных системах;
- использовать типовые криптографические средства защиты информации;
- применять методы и средства защиты от вредоносных программ.

В результате освоения учебной дисциплины обучающийся должен знать**:**

- место и роль информационной безопасности в системе национальной безопасности Российской Федерации;
- основные нормативные правовые акты в области информационной безопасности и защиты информации;
- сущность и понятие информационной безопасности и защиты информации;
- источники возникновения информационных угроз;
- методы антивирусной защиты информации;
- методы криптографического преобразования информации;
- терминологию, применяемую в специальной литературе по профилю работы.

1.4. Количество часов на освоение рабочей программы учебной дисциплины:

максимальной учебной нагрузки обучающегося **95** часов, в том числе:
обязательной аудиторной учебной нагрузки обучающегося **63** часа;
самостоятельной работы 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)	*95*
Обязательная аудиторная учебная нагрузка (всего)	*63*
в том числе:	
лабораторные работы	*
практические занятия	*30*
контрольные работы	*
курсовая работа (проект) (*если предусмотрено)*	*
Самостоятельная работа обучающегося (всего)	*32*
в том числе:	
самостоятельная работа над курсовой работой (проектом) *(если предусмотрено)*	*
внеаудиторная самостоятельная работа: *работа над конспектом лекций;* *работа с учебниками и учебными пособиями;* *выполнение индивидуальных заданий, поиск информации в сети Интернет, подготовка материала для исследовательской (проектной) деятельности (по тематике самостоятельной работы);* *подготовка к практическим занятиям, оформление отчетов по выполненным работам.*	*32*
Промежуточная аттестация в форме:	*экзамена*

2.2. Тематический план и содержание учебной дисциплины ОП.11 «Информационная безопасность»

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. Актуальность проблемы обеспечения безопасности информации			**6**	
Тема 1.1 Концепция информационной безопасности	**Содержание учебного материала**		***2***	
	1	Содержание дисциплины и ее задачи. Связь с другими дисциплинами. Концептуальная модель информационной безопасности. Информационная безопасность в системе национальной безопасности Российской Федерации.	2	1
	Практические занятия			
	Самостоятельная работа обучающихся: Работа с конспектом лекции. Проект - Информационная безопасность		2	
Тема 1.2 Составляющие и аспекты информационной безопасности	**Содержание учебного материала**		***2***	
	1	Предмет и объект защиты. Задачи, методы и средства обеспечения информационной безопасности. (конфиденциальность, целостность, доступность).	2	2
	Практические занятия			
	Самостоятельная работа обучающихся: Работа с конспектом лекции. Проект - Информационная безопасность		1	
Тема 1.3 Угрозы информационной безопасности	**Содержание учебного материала**		***2***	
	1	Понятие надежности и уязвимости информации. Понятие угрозы. Виды угроз информационной безопасности, источники и содержание угроз в информационной сфере. Классификация случайных и преднамеренных угроз. Обнаружение и противодействие атакам. Методы и средства предотвращения случайных угроз КС	2	2
	Практические занятия			

	Самостоятельная работа обучающихся: Работа с конспектом лекции. Подготовка сообщения «Наиболее распространенные угрозы информационной безопасности».		2	
Раздел 2. Способы и методы защиты информационных ресурсов			**32**	
Тема 2.1 Основные понятия защиты информации и информационной безопасности.	**Содержание учебного материала**		***2***	
	1	Защита информации как одно из направлений обеспечения информационной безопасности. Основные концептуальные положения системы защиты информации. Эффективность защиты информации. Защита информации от утечки, от разглашения. Классификация средств защиты информации.	2	2
	Практические занятия		***2***	
	№1	Разграничение прав пользователей в защищённых версиях операционной системы Windows	2	
	Самостоятельная работа обучающихся: Работа с конспектом лекции.		1	
Тема 2.2 Защита информации от несанкционированного доступа	**Содержание учебного материала**		***2***	
	1	Причины несанкционированного доступа к информации. Каналы несанкционированного воздействия. Последствия несанкционированного доступа к информации. Защита информации от несанкционированного доступа.	2	
	Практические занятия		***4***	
	№2	Разграничение доступа к ресурсам в защищённых версиях операционной системы Windows	2	
	№3	Основы использования средств защиты от НСД в операционной системе Linux	2	
	Самостоятельная работа обучающихся: Работа с конспектом лекции.		1	
Тема 2.3 Защита информации в компьютерных системах	**Содержание учебного материала**		***2***	
	1	Современные средства идентификации и аутентификации, разграничение доступа, аудит, шифрование, контроль целостности. Пароли заставки экрана, удаленного доступа, включения. Сетевая защита паролями. Программное обеспечение для защиты паролем (обзор). Разграничение полномочий и управление доступом к ресурсам в защищенных версиях ОС Windows. Биометрические методы защиты.	2	2

	Практические занятия		***2***	
	№4	Назначение прав пользователей при произвольном управлении доступом в Windows	2	
	Самостоятельная работа обучающихся: Составление презентаций, рефератов, сообщений. Примерная тематика презентаций, докладов: - «Контроль правильности функционирования системы защиты». - Биометрические методы защиты, их сравнительная характеристика.		3	
Тема 2.4. Концепция безопасности реляционных баз данных	**Содержание учебного материала**		***2***	
	1	Угрозы безопасности БД: общие и специфические. Требования безопасности БД. Защита от несанкционированного доступа (НСД). Защита от вывода. Целостность БД. Аудит. Задачи и средства администратора безопасности баз данных. Многоуровневая защита.	2	2
	Практические занятия		***2***	
	№5	Настройка параметров аутентификации Windows	2	
	Самостоятельная работа обучающихся: Работа с конспектом лекции.		2	
Тема 2.5. Организационные, правовые средства защиты информации от несанкционированного доступа	**Содержание учебного материала**		***2***	
	1	Концепция правового обеспечения информационной безопасности Российской Федерации. Законодательная база, стандарты, нормативно-методические документы РФ в области обеспечения информационной безопасности. Ответственность за нарушения законодательства в информационной сфере. Зарубежные стандарты и международные соглашения в области информационной безопасности. Международное сотрудничество в области борьбы с компьютерной преступностью	2	2
	Практические занятия		***6***	
	№6	Аудит ресурсов и событий	4	
	№7	Реализация политики безопасности в защищённых версиях операционной системы Windows	2	
	Самостоятельная работа обучающихся: Работа с конспектом лекции.		2	
	Содержание учебного материала		***2***	
	2	Понятие о правовых средствах защиты информации. Законы, регулирующие деятельность по защите информации. Правовой режим защиты государственной тайны, конфиденциальной информации. Организационная защита информации и её место в системе комплексной защиты информации в информационной системе. Порядок создания, утверждения и исполнения должностных инструкций	2	2

	Практические занятия:			
	Самостоятельная работа обучающихся: Проект - Организационно-правовое обеспечение информационной безопасности. Работа с учебниками и учебными пособиями по теме «Государственная тайна», «Коммерческая тайна», «Банковская тайна», «Профессиональная тайна», «Служебная тайна», «Охрана интеллектуальной собственности» и др. Составление презентаций, рефератов, сообщений.		2	
Тема 2.6. Криптографические методы и средства обеспечения информационной безопасности.	**Содержание учебного материала**		***2***	
	1	Понятие криптологии, как научного направления защиты информации. Основные понятия. Криптографические механизмы конфиденциальности, целостности и аутентичности информации. Виды и алгоритмы криптографической защиты. Симметричные и ассиметричные криптосистемы. Обеспечение целостности информации на основе электронной цифровой подписи. Виды компьютерной стеганографии.	2	2
	Практическое занятие		***2***	
	№8	Криптографические методы защиты информации. Шифрующая файловая система EFS и управление сертификатами в Windows	2	
	Самостоятельная работа обучающихся: Работа с учебниками и учебными пособиями по теме «Характеристики криптографических средств защиты. Индивидуальное задание: шифры перестановки, шифры простой замены, шифры сложной замены.		2	
Раздел 3. Борьба с вирусным заражением информации			***22***	
Тема 3.1. Проблема вирусного заражения и структура современных вирусов.	**Содержание учебного материала**		***2***	
	1	Понятие об опасных и вредоносных программах. Характеристика компьютерной программы как вида информационного нарушителя. Угроза вирусов безопасности информации. Классификация компьютерных вирусов. Основные этапы жизненного цикла вирусов. Объекты внедрения, режимы функционирования и специальные функции вирусов. Схемы заражения файлов. Способы маскировки, используемые вирусами.	2	2

	Практические занятия			
	Самостоятельная работа обучающихся: Изучение литературы по теме: Компьютерные вирусы. Структура современных вирусов Создание классификации вирусов в программе FreeMind.		3	
Тема 3.2. Программные закладки	**Содержание учебного материала**		***2***	
	1	Классификация «вирусоподобных» программ (закладок). Модели воздействия программных закладок на компьютеры. Методы защиты от программных закладок	2	2
	Практические занятия		***2***	
	№9	Основные признаки присутствия на компьютере вредоносных программ	2	
	Самостоятельная работа обучающихся: Изучение литературы по теме «Средства вторжения в частную жизнь».		2	
Тема 3.3. Защита от компьютерных вирусов. Антивирусные программы	**Содержание учебного материала**		***2***	
	1	Основные организационные и программные меры антивирусной защиты. Обзор антивирусных программ. Методика использования антивирусных программ. Восстановление пораженных компьютерными вирусами объектов. Условия безопасной работы КС и технология обнаружения заражения вирусами. Основные организационные и программные меры антивирусной защиты.	2	2
	Практические занятия		***2***	
	№10	Защита от несанкционированного доступа и сетевых хакерских атак. Функционал и настройки антивирусных программ	2	
	Самостоятельная работа обучающихся: Проект - Защита от вредоносных программ-закладок		3	
Тема 3.4. Сетевая безопасность	**Содержание учебного материала**		***2***	
	1	Угрозы информации в компьютерных сетях. Действия компьютерных вирусов и программных закладок в сетях ЭВМ. Троянские программы.	2	2
	Практические занятия		***4***	
	№11	Выявление вредоносных программ с помощью реестра Windows. Профилактика проникновения «троянских программ»	2	
	№12	Изучение штатных средств ОС Windows, предназначенных для обеспечения ИБ при использовании глобальных вычислительных сетей	2	
	Самостоятельная работа обучающихся: Подготовка сообщения по теме «Каналы несанкционированного получения информации в		2	

	АСОД»			
Тема 3.5. Опасности работы с электронной почтой	**Содержание учебного материала**		***2***	
	1	Угрозы конфиденциальности электронной почты. Возможность перехвата электронной почты. Оценка эффективности шифрования.	2	2
	Практические занятия		***4***	
	№13	Способы первичной защиты компьютера. Опасности работы с электронной почтой	2	
	№14	Управление шаблонами безопасности в Windows	2	
	Самостоятельная работа обучающихся: Подбор материала к практическим занятиям.		2	
Раздел 4. Организационно-правовое обеспечение информационной безопасности			**3**	
Тема 4.1. Концепция правового обеспечения информационной безопасности РФ	**Содержание учебного материала**		***2***	
	1	Законы, регулирующие деятельность по защите информации, их основные положения. Государственная политика обеспечения информационной безопасности РФ. Защита человека и гражданина от неинформированности. Отечественные и зарубежные стандарты в области информационной безопасности. Стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий». Руководящие документы Гостехкомиссии России.	2	2
	Практические занятия			
	Самостоятельная работа обучающихся: Подготовка сообщений по вопросу «Международные правовые акты по защите информации».		2	
Тема 4.2. Ответственность за нарушение законодательства в информационной сфере	**Содержание учебного материала**		***1***	
	1	Развитие законодательства в сфере противодействия преступлениям связанным с компьютерной информацией. Уголовно-правовая характеристика преступлений в сфере компьютерной информации.	1	2
	Практические занятия			
	Самостоятельная работа обучающихся: Подбор материала и подготовка презентаций и докладов по направлениям: - по вопросам ответственности за компьютерные преступления; - по политике информационной безопасности.		2	

Всего:	**63**	лекц. – **33** практ. – **30** самост. – **32**

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 учебной дисциплины требует наличия учебного кабинета; лаборатории информационно-коммуникационных систем.

3.1.1. Оборудование кабинета и рабочих мест кабинета:

- рабочее место преподавателя,
- учебная мебель по количеству обучающихся,
- учебная доска;
- мультимедиа комплекс (компьютер, мультимедийный проектор, экран),
- локальная сеть, выход в Интернет;
- лицензионное программное обеспечение;
- наглядные пособия (учебники, презентации, интерактивные плакаты, раздаточный материал, комплекты МУ для выполнения практических работ)

3.1.2. Технические средства обучения:

- мультимедиа комплекс (компьютер, мультимедийный проектор, экран);
- компьютеры (по количеству обучающихся с лицензионным программным обеспечением);
- сервер;
- локальная сеть;
- выход в Интернет;
- принтер черно-белый лазерный;
- комплект учебно-методической документации.

3.1.3. Оборудование лаборатории и рабочих мест лаборатории:

- персональные компьютеры с лицензионным программным обеспечением;
- сервер;
- локальная сеть;

- выход в Интернет;
- мультимедиа комплекс (компьютер, мультимедийный проектор, экран);
- рабочее место преподавателя (ПК, сканер, принтер);
- рабочая немеловая доска.

3.1.4. Действующая нормативно-техническая и технологическая документация:

- правила техники безопасности и противопожарной безопасности;
- инструкции по эксплуатации компьютерной техники и правила работы в лаборатории информационно-коммуникационных систем;
- Положение о лаборатории информационно-коммуникационных.

3.1.5. Программное обеспечение:

- ОС Windows 7;
- MS Office 2007;
- современные антивирусные программные продукты;
- программа Free Mind;
- интегрированные приложения для работы в Интернете Microsoft Internet Explorer, Opera и др.;
- программы шифрования данных, в том числе программы шифрования по ГОСТ 28147-89, DES и RSA;
- файл-образ загрузочного диска ОС Windows 7;
- программа VM Oracle VirtualBox.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, дополнительной литературы, Интернет-ресурсов

Основные источники:

1. Доктрина информационной безопасности Российской Федерации. (утв. Президентом РФ 9 сентября 2000 г. № Пр-1895).
2. Закон РФ от 5 мая 1992 года № 2446-1 «О безопасности».

3. Закон РФ от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
4. ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.
5. ГОСТ Р 50922-96. Защита информации. Основные требования и определения.
6. ОСТ 45.127-99. Система обеспечения информационной безопасности взаимоувязанной сети связи РФ. Термины и определения.
7. Партыка Т. Л., Попов И.И. Информационная безопасность. Учебное пособие для студентов учреждений среднего профессионального образования. - М: ФОРУМ: ИНФРА- М, 2011.
8. Мельников В.П. Информационная безопасность и защита информации: учеб. пособие, 6 издание /В.П.Мельников, С.А. Клейменов, А.П.Петраков; под ред. С.А. Клейменова. – М.: Академия, 2011.
9. Мельников В.П. Информационная безопасность. Практикум. - ОИЦ "Академия", 2010.

Дополнительные источники:

1. Мельников В.П. Информационная безопасность. - ОИЦ "Академия", 2008
2. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – Изд-во: ДМК Пресс, 2012.
3. Расторгуев С.П. Основы информационной безопасности. – М.: Академия, 2007.
4. Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации. – М.: Академия, 2010.
5. Гришина Н.В. Комплексная система защиты информации на предприятии. - М.: Форум, 2009.
6. Хорев П.Б. Методы и средства защиты информации в компьютерных системах. – М.: Академия, 2006.

Интернет-ресурсы и источники

1. Интернет-портал www.sciyouth.ru.
2. Интернет Университет Информационных технологий [Электронный ресурс]

– Режим доступа: www.intuit.ru.

3. Каталог библиотеки учебных курсов - Режим доступа: http://msdn.microsoft.com/ru-ru/gg638594

4. Сетевая энциклопедия Википедия [Электронный ресурс] – Режим доступа: http://ru.wikipedia.org.

5. Федеральный портал «Информационно-коммуникационные технологии в образовании» [Электронный ресурс] – Режим доступа: http://window.edu.ru.

6. Федеральный портал «Российское образование» [Электронный ресурс] – Режим доступа: http:// www.edu.ru

7. http://www.ict.edu.ru/catalog/index.php

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

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

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
Усвоение знаний	
Сущность информационной безопасности информационных систем	Тестирование по теме «Понятие информационной безопасности». Защита презентаций, рефератов, сообщений. Методы - наблюдение, практический контроль
Состав и методы организационно- правовой защиты информации.	Защита отчёта практического занятия по изучению нормативных и правовых документов защиты информации. Защита презентаций, рефератов, сообщений. Методы - наблюдение, практический контроль.
Источники возникновения информационных угроз.	Тестирование по теме «Угрозы безопасности». Защита презентаций, рефератов, сообщений. Методы - наблюдение, практический контроль.
Методы антивирусной защиты информации.	Тестирование по теме «Антивирусная защита информации». Защита презентаций, рефератов, сообщений. Методы - наблюдение, практический контроль
Протоколы идентификации и проверки подлинности пользователя.	Тестирование по теме «Идентификация и проверка подлинности пользователя». Защита презентаций, рефератов, сообщений. Методы - наблюдение, практический контроль
Процедуры аутентификации данных и постановки электронной цифровой подписи.	Тестирование по теме «Электронная цифровая подпись». Защита презентаций, рефератов, сообщений. Методы - наблюдение, практический контроль
Освоение умений	
Применять правовые, организационные, технические, программные средства защиты информации.	Защита отчётов практических занятий по разработке организационных мероприятий и должностных инструкций сотрудников отдела информационной безопасности информационной системы. Методы - наблюдение, практический контроль
Применять методы и средства защиты от вредоносных программ.	Защита отчёта практической работы по изучению современных методов антивирусной защиты информации. Методы - наблюдение, практический контроль
Применять методы разграничения полномочий пользователей и управления досту-	Защита отчётов практических работ по управлению учетными записями пользователей, по

пом к ресурсам в защищенных операционных системах	реализация политики безопасности. Методы - наблюдение, практический контроль
Использовать типовые криптографические средства защиты информации.	Защита отчётов практических занятий по изучению традиционных криптосистем. Методы - наблюдение, практический контроль

Разработчик:

ГБПОУ «ПХТТ»	преподаватель	В.Е. Котельникова
(место работы)	(занимаемая должность)	(инициалы, фамилия)