

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

**Орский гуманитарно-технологический институт (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования**

**«Оренбургский государственный университет»
(Орский гуманитарно-технологический институт (филиал) ОГУ)**

Факультет среднего профессионального образования

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«ОП.17 Информационная безопасность на предприятии»

Специальность

09.02.07 Информационные системы и программирование
(код и наименование специальности)

Тип образовательной программы

Программа подготовки специалистов среднего звена

Квалификация

специалист по информационным системам

Форма обучения

очная

Рабочая программа дисциплины «ОП.17 Информационная безопасность на предприятии» /сост. М.А. Кузниченко – Орск: Орский гуманитарно-технологический институт (филиал) ОГУ, 2022.

Рабочая программа предназначена для преподавания дисциплины общепрофессионального цикла студентам очной формы обучения по специальности 09.02.07 Информационные системы и программирование в 8 семестре.

Рабочая программа составлена с учетом Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.07 Информационные системы и программирование, утвержденного приказом Министерства образования и науки Российской Федерации от "09" декабря 2016 г. № 1547.

Содержание

1 Цели и задачи освоения дисциплины	4
2 Место дисциплины в структуре ППСЗ	4
3 Требования к результатам освоения содержания дисциплины	4
4 Организационно-методические данные дисциплины	5
5 Содержание и структура дисциплины	5
5.1 Содержание разделов дисциплины	5
5.2 Структура дисциплины	6
5.4 Темы рефератов	7
5.5 Самостоятельная работа	7
6 Организация текущего контроля	8
7 Образовательные технологии	8
7.1 Интерактивные образовательные технологии, используемые в аудиторных занятиях	8
8 Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов	9
9 Учебно-методическое обеспечение дисциплины	9
9.1 Рекомендуемая литература	9
9.1.1 Основная литература	9
9.1.2 Дополнительная литература	9
9.1.3 Периодические издания	9
9.1.4 Интернет-ресурсы	10
9.2 Средства обеспечения освоения дисциплины	10
9.2.1 Методические указания и материалы к лабораторным занятиям и самостоятельной работе	10
10 Материально-техническое обеспечение дисциплины	11

1 Цели и задачи освоения дисциплины

Целями освоения дисциплины «Информационная безопасность на предприятии» являются развитие у студентов личностных качеств, а также формирование общих и профессиональных компетенций в соответствии с требованиями ФГОС СПО по специальности 09.02.07 Информационные системы и программирование.

2 Место дисциплины в структуре ПСССЗ

Учебная дисциплина «Информационная безопасность на предприятии» входит в состав общепрофессионального цикла учебного плана специальности, где она содержательно-методически взаимосвязана с дисциплинами «Программные решения для бизнеса», «IT-решения для бизнеса на платформе 1С: Предприятие 8», «Правовое обеспечение профессиональной деятельности».

Для изучения данной дисциплины необходимо знать такие дисциплины: «Информационные технологии», «Инструментальные средства разработки программного обеспечения», «Управление проектами», «Разработка кода информационных систем».

Освоение данной дисциплины необходимо как предшествующее для дипломного проектирования.

Навыки, полученные в результате освоения дисциплины «Информационная безопасность на предприятии» будут необходимы при прохождении преддипломной практики.

3 Требования к результатам освоения содержания дисциплины

Процесс изучения дисциплины «Информационная безопасность на предприятии» направлен на формирование у обучающихся элементов следующих общих и профессиональных компетенций в соответствии с ФГОС СПО по данному направлению:

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

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

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

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

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

ОК 09. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.

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

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

Знать:

- угрозы информационной безопасности
- средства защиты компьютерной информации
- технология установки и настройки сервера баз данных.
- требования к безопасности сервера базы данных.
- государственные стандарты и требования к обслуживанию баз данных.

Уметь:

- проводить анализ угроз информационной безопасности;
- выполнять основные этапы решения задач информационной безопасности;

- применять стандартные методы для защиты объектов базы данных;
- применять на практике основные общеметодологические принципы информационной безопасности
- использовать стандартные методы защиты объектов базы данных
- Разрабатывать политику безопасности SQL сервера, базы данных и отдельных объектов базы данных.

4 Организационно-методические данные дисциплины

Общее количество часов дисциплины составляет 72 часа

Вид работы	Количество часов по учебному плану	
	8 семестр	Всего
Лекции, уроки	23	23
Практические занятия, семинары	-	-
Лабораторные занятия	30	30
Консультации	1	1
Промежуточная аттестация	9	9
Самостоятельная работа	9	9
Форма промежуточной аттестации		экзамен

5 Содержание и структура дисциплины

5.1 Содержание разделов дисциплины

Наименование раздела и темы	Содержание
Раздел 1 Основы информационной безопасности в информационных системах	
Тема 1.1.	Понятие информационной безопасности (ИБ). Составляющие ИБ: конфиденциальность, доступность, целостность. Защита информации.
Тема 1.2.	Основные понятия и определения, эволюция подходов к обеспечению информационной безопасности.
Тема 1.3.	Угрозы ИБ, классификация угроз ИБ. Угроза безопасности информации в компьютерных системах.
Раздел 2 Уровни обеспечения информационной безопасности	
Тема 2.1	Законодательный уровень. Комплексное обеспечение ИБ. Уровни обеспечения ИБ. Меры ограничительной направленности; направляющие и координирующие меры.
Тема 2.2	Обзор российского законодательства в области информационной безопасности. Компьютерные преступления, мера ответственности.
Тема 2.3	Цифровая подпись офисных документов.
Тема 2.4	Парольная защита файла БД.
Тема 2.5	Особенности административного уровня защиты информации. Политика безопасности.
Тема 2.6	Идентификация и аутентификация пользователей. Парольная защита. Идентификация и аутентификация с помощью биометрических данных

Наименование раздела и темы	Содержание
Раздел 3 Вредоносное программное обеспечение и защита от него	
Тема 3.1	История появления компьютерных вирусов. Классификация вредоносного ПО. Признаки заражения компьютерными вирусами.
Тема 3.2	Антивирусные программы. Современные технологии борьбы с вирусами.

5.2 Структура дисциплины

Разделы дисциплины «Основы проектирования баз данных», изучаемые в 8 семестре

№ раздела	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Внеауд. работа СР
			ЛК	ПЗ	ЛЗ	
1	Основы информационной безопасности в информационных системах	9	6	-	0	3
2	Уровни обеспечения информационной безопасности	35	12	-	20	3
3	Вредоносное программное обеспечение и защита от него	18	5	-	10	3
	Консультация	1				
	Промежуточная аттестация	9				
	Итого:	72	23	-	30	9

5.4 Лабораторные занятия

№ занятия	№ раздела	Тема	Кол-во часов
1.	2	Защита ячеек и файла MS Excel	2
2.	2	Цифровая подпись офисных документов.	2
3.	2	Парольная защита файла БД MS Access	2
4.	2	Защита текстового документа от копирования после скачивания	2
5.	2	Генерация пароля пользователя случайным образом.	2
6.	2	Сохранение логина и пароля пользователя в БД. Аутентификация пользователя	2
7.	2	Настройка браузера для защиты от спама	2
8.	2	Создание презентаций рефератов по ИБ.	2
9.	2	Методы криптографического преобразования данных.	2

№ занятия	№ раздела	Тема	Кол-во часов
10.	2	Аппаратное шифрование и программные пакеты для шифрования.	
11.	3	Классификация вирусов	2
12.	3	Вред, наносимый информации компьютерными вирусами.	2
13.	3	Программы антивирусной защиты	2
14.	3	Методы защиты от вирусов Антивирусное ПО.	2
15.	3	Защита лабораторных работ	2
		Итого:	30

5.4 Темы рефератов

Список тем рефератов	
<ol style="list-style-type: none"> 1. Преступления в сфере компьютерной информации 2. Защита почтовых сообщений 3. Компьютерная преступность и компьютерная безопасность 4. Компьютерные вирусы: история, классификация, признаки 5. Антивирусная защита 6. Правовые информационные системы: сравнительный анализ 7. Шифрование информации 8. Криптография: история развития 9. Криптографические системы защиты данных 10. Стеганография. Становление как науки. Компьютерная стеганография и её применение 11. Туннелирование. Управление. Обеспечение отказоустойчивости и обслуживаемости 12. Виды спама и нежелательного контента, методы и средства борьбы с ними 13. Международное и национальное законодательство о работе сети Интернет 14. Защита информации в сети Интернет 15. Правовая основа информационной безопасности в России и в мире 16. Электронная цифровая подпись 17. Информационная безопасность электронной коммерции 18. Настройка безопасности ОС Windows при работе в сети 19. Несанкционированный доступ к сети WiFi 20. Спам и нормы пользования сетью 	

5.5 Самостоятельная работа

№ раздела	Тема	Кол-во часов
1	Правовые информационные системы: ГАРАНТ, КонсультантПлюс	3
2	Одноключевые (симметричные, с секретным ключом) системы шифрования	3
3	Современные антивирусные программы	3

№ раздела	Тема	Кол-во часов
	Итого	9

Основы информационной безопасности в информационных системах
Уровни обеспечения информационной безопасности
Вредоносное программное обеспечение и защита от него

6 Организация текущего контроля

Вид занятия	Номер контр. точки	Разделы рабочей программы, подлежащие контролю			Форма контроля	Сроки проведения
		1	2	3		
Л, ЛЗ	1	*			Устный опрос	Согласно КТП
	2		*		Тест	Согласно КТП
	3			*	Тест	Согласно КТП

7 Образовательные технологии

- обучение в сотрудничестве;
- использование ресурсов сети Internet;
- технология разноуровневого обучения;
- личностно-ориентированный подход;
- использование алгоритмов и опорных конспектов;
- информационные технологии;
- внеаудиторная работа.

7.1 Интерактивные образовательные технологии, используемые в аудиторных занятиях

Номер раздела	Используемая интерактивная образовательная технология	Количество часов
1	Презентации «Информационная безопасность» - базовые понятия и определения	2
1	Мир в цифрах. ИБ. (1мин) https://www.youtube.com/watch?v=22xwDm7Nw_0	1
2	Жестокие будни компьютерной криминалистики (телепередача 37 мин) https://www.youtube.com/watch?v=h8qg_OK_26k	1
2	Видео сюжет «Охота на хакера – виртуальные ограбления» https://www.youtube.com/watch?v=QGMq9JG8jEo	1
3	Поиск в сети Интернет сведений об антивирусном ПО	1
4	Видео: Хакеры (Анонимус) секретный документальный фильм , Анна Чапман (43 мин) https://www.youtube.com/watch?v=VRX3-Av3Btg	1
Итого:		7

8 Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Код контролируемого результата обучения	Оценочное средство
ОК 01. ОК 02. ОК 03. ОК 04. ОК 05. ОК 09. ОК 10. ПК 5.3 ПК 7.5	<i>Тестирование, контрольные работы, устные опросы, проверка домашних работ, защита лабораторных работ</i>

9 Учебно-методическое обеспечение дисциплины

9.1 Рекомендуемая литература

9.1.1 Основная литература

1. Бубнов А.А. Основы информационной безопасности: учебное пособие для студ. учреждений сред. проф. образования. – М.: Издательский центр «Академия», 2015. – 256 с.
2. Попов И.И. Информационная безопасность : учеб. пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2018. — 432 с. — (Среднее профессиональное образование). - Режим доступа: <http://znanium.com/catalog/product/915902>
3. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 432 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-473-1. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1189328> – Режим доступа: по подписке.

9.1.2 Дополнительная литература

4. Гришина Н.В. Информационная безопасность предприятия : учеб. пособие / Н.В. Гришина. — 2-е изд., доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 239 с. : ил. — (Высшее образование: Бакалавриат). - Режим доступа: <http://znanium.com/catalog/product/612572>
5. Мещатунян М.В. Основные положения информационной безопасности : учеб. пособие / В.Я. Ищейнов, М.В. Мещатунян. — М. : ФОРУМ : ИНФРА-М, 2018. — 208 с. — (Среднее профессиональное образование). - Режим доступа: <http://znanium.com/catalog/product/927190>

9.1.3 Периодические издания

1. Chip с DVD / Чип с DVD
2. LINUX FORMAT (ЛИНУКС ФОРМАТ) + DVD-приложение
3. PC MAGAZINE / RE. Персональный компьютер сегодня
4. Вестник компьютерных и информационных технологий
5. Вы и ваш компьютер
6. Журнал сетевых решений/ LAN

9.1.4 Интернет-ресурсы

- 1 ЭБС «Электронная библиотека онлайн» – <http://www.biblioclub.ru/>
- 2 ЭБС Znanium.com – <http://znanium.com/>
- 3 Ежемесячный компьютерный журнал КомпьютерПресс – <http://www.compress.ru>

9.2 Средства обеспечения освоения дисциплины

9.2.1 Методические указания и материалы к лабораторным занятиям и самостоятельной работе

Методические указания к лабораторным работам, дидактический и наглядный материал

9.2.2 Программное обеспечение, профессиональные базы данных и информационные справочные системы современных информационных технологий

Тип программного обеспечения	Наименование	Схема лицензирования, режим доступа
Операционная система	Microsoft Windows	Подписка Open Value Subscription – Education Solutions (OVS-ES) по договору: № 8В/21 от 15.06.2021 г.
Офисный пакет	Microsoft Office	
Интернет-браузер	Internet Explorer	Является компонентом операционной системы Microsoft Windows
	Opera	Бесплатное ПО, http://www.opera.com/ru/terms
	Mozilla Firefox	Свободное ПО, https://www.mozilla.org/en-US/foundation/licensing/
	Google Chrome	Бесплатное ПО, http://www.google.com/intl/ru/policies/terms/
Мультимедийный плеер	Windows Media Player	Является компонентом операционной системы Microsoft Windows
Векторный графический редактор, редактор диаграмм и блок-схем	Microsoft Visio Standard 2007	Сертификат Microsoft Open License № 46284547 от 18.12.2009 г., академическая лицензия на рабочее место
Информационно-правовая система	Консультант Плюс	Комплект для образовательных учреждений по договору № 337/12 от 04.10.2012 г., сетевой доступ
Интегрированная среда разработки программного обеспечения	PascalABC.NET	Свободное ПО, http://www.pascalabc.net/litsenzionnoe-soglashenie
	Embarcadero RAD Studio 2010 Professional	Образовательная лицензия по государственному контракту № 32/09 от 17.12.2009 г., сетевой конкурентный доступ
	Dev-C++	Свободное ПО, http://www.gnu.org/licenses/gpl.html

9.2.3 Критерии оценки формы контроля промежуточной аттестации

Форма итогового контроля знаний и умений по дисциплине «Информационная безопасность на предприятии» – экзамен. К экзамену допускаются обучающиеся, выполнившие все лабораторные задания и получившие положительные оценки за все проводимые проверочные работы.

Обучающийся получает оценку:

«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.

10 Материально-техническое обеспечение дисциплины

Для реализации программы учебной дисциплины «Информационная безопасность на предприятии» предусмотрена лаборатория «Программного обеспечения и сопровождения компьютерных систем», оснащённая автоматизированными рабочими местами на 12-15 обучающихся (процессор не ниже Core i3, оперативная память объемом не менее 4 Гб) или аналоги, автоматизированным рабочим местом преподавателя (процессор не ниже Core i3, оперативная память объемом не менее 4 Гб) или аналоги, 12-15 комплектов компьютерных комплектующих для производства сборки, разборки и сервисного обслуживания ПК и оргтехники, специализированной мебелью для сервисного обслуживания ПК с заземлением и защитой от статического напряжения, многофункциональным устройством (МФУ) формата А4.

