Автономная некоммерческая организация профессионального образования

«ВЕРХНЕВОЛЖСКИЙ МЕЖОТРАСЛЕВОЙ ТЕХНИКУМ»

УТВРЖДАЮ
Директор Верхневолжского
межотраслевого техникума

А.И. Садыкова

«29» января 2025 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.14 Информационная безопасность

программы подготовки специалистов среднего звена
по специальности
09.02.07 Информационные системы и программирование

Программист

квалификация

Составитель:

Фамилия, имя, отчество	Должность
Бондарь И.В.	преподаватель

Рабочая программа учебного предмета разработана на основе требований:

федерального государственного образовательного стандарта среднего общего образования, утвержденного приказом Министерства образования и науки Российской Федерации от 17 мая 2012 г. № 413 (далее – ФГОС СОО),

федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.07 Информационные системы и программирование, утвержденного приказом Министерства образования и науки РФ от 9 декабря 2016 г. №1547 (далее – ФГОС СПО),

Федеральной образовательной программы среднего общего образования, утвержденной приказом Министерства просвещения Российской Федерации от 18.05.2023 № 371, с учетом получаемой специальности.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ОП.14. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1.1. Область применения программы

Рабочая программа учебной дисциплины является частью образовательной программы в соответствии с ФГОС по специальности СПО 09.02.07 Информационные системы и программирование.

1.2. Место дисциплины в структуре образовательной программы:

Учебная дисциплина ОП.14. Информационная безопасность принадлежит к общепрофессиональному циклу.

В результате освоения образовательной программы у выпускника должны быть сформированы общие и профессиональные компетенции.

Выпускник, освоивший образовательную программу, должен обладать следующими компетенциями:

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.;

ПК 1.4. Выполнять тестирование программных модулей.;

ПК 11.5. Администрировать базы данных.;

ПК 11.6. Защищать информацию в базе данных с использованием технологии защиты информации.

1.3. Цели и задачи дисциплины - требования к результатам освоения дисциплины:

Цель изучения дисциплины - защита национальных интересов; обеспечение человека и общества достоверной и полной информацией; правовая защита человека и общества при получении, распространении и использовании информации.

Задачами являются: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией.

В результате освоения дисциплины студент *должен знать:*

- основные средства и методы защиты компьютерных систем программными и аппаратными средствами;
- 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.

В результате освоения дисциплины студент *должен 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.

1.4. Количество часов на освоение программы дисциплины: Объем образовательной программы - **46** часов, в том числе:
Занятия во взаимодействии с преподавателем - 36 часов; самостоятельной работы обучающегося - 10 часов.
Форма итоговой аттестации: дифференцированный зачет

При угрозе возникновения и (или) возникновении отдельных чрезвычайных ситуаций, введении режима повышенной готовности или чрезвычайной ситуации на всей территории Российской Федерации либо на ее части реализация рабочей программы учебной дисциплины может осуществляться с применением электронного обучения, дистанционных образовательных технологий.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Объем образовательной программы	**46**
Занятия во взаимодействии с преподавателем	**36**
в том числе:	
теоретические занятия	14
лабораторные занятия *(не предусмотрены)*	-
практические занятия	20
контрольные работы *(не предусмотрены)*	-
курсовая работа (проект) *(не предусмотрен)*	-
Самостоятельная работа обучающегося (всего)	**10**
в том числе:	
самостоятельная работа над курсовой работой (проектом) *(не предусмотрено)*	-
Итоговая аттестация в форме дифференцированного зачета	2

2.2. Тематический план и содержание учебной дисциплины ОП.14. Информационная безопасность

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся, курсовая работ (проект) *(если предусмотрен ы)*		Объем в часах	Коды компетенций, формировани ю которых способствует элемент программы
1	***2***		**3**	***4***
Раздел 1. Борьба с угрозами несанкционированного доступа к информации				
Тема 1.1. Актуальность проблемы обеспечения безопасности информации Безопасность БД, угрозы, защита	**Содержание учебного материала**		**2**	
	1	Основные понятия безопасности: конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации. Возможные угрозы информационной безопасности: классификация, источники возникновения и пути реализации. Виды угроз. Определение требований к уровню обеспечения информационной безопасности. Управление рисками. Основные понятия. Процесс оценки рисков. Понятие безопасности БД. Угрозы безопасности БД: общие и специфичные. Требования безопасности БД. История развития, назначение и роль баз данных. Модели данных. Математические основы построения реляционных СУБД	2	ОК 01., ОК 02., ОК 04., ОК 05., ОК 09., ПК 1.4., ПК 11.5., ПК 11.6.
	Лабораторные работы *(не предусмотрены)*		-	
	Практические занятия		**4**	
	1	Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Работа с содержанием нормативных правовых актов	2	
	2	Анализ рисков информационной безопасности	2	

	Контрольные работы *(не предусмотрены)*		-	
	Внеаудиторная самостоятельная работа обучающихся		**2**	
	1	Доклад на тему: «Защита информации, тайна»	2	
Тема 1.2. Критерии защищенности БД	**Содержание учебного материала**		**1**	ОК 01., ОК 02., ОК 04., ОК 05., ОК 09., ПК 1.4., ПК 11.5., ПК 11.6.
	1	Критерии оценки надежных компьютерных систем (TCSEC). Понятие политики безопасности. Совместное применение различных политик безопасности в рамках единой модели. Интерпретация TCSEC для надежных СУБД (TDI). Оценка надежности СУБД как компоненты вычислительной системы.	1	
	Лабораторные работы *(не предусмотрены)*		-	
	Практическое занятие *(не предусмотрены)*		-	
	Контрольные работы *(не предусмотрены)*		-	
	Внеаудиторная самостоятельная работа обучающихся *(не предусмотрены)*		**-**	
Тема 1.3. Модели безопасности в СУБД	**Содержание учебного материала**		**1**	ОК 01., ОК 02., ОК 04., ОК 05., ОК 09., ПК 1.4., ПК 11.5., ПК 11.6.
	1	Дискреционная (избирательная) и мандатная (полномочная) модели безопасности. Классификация моделей. Аспекты исследования моделей безопасности. Особенности применения моделей безопасности в СУБД.	1	
	Лабораторные работы *(не предусмотрены)*		-	
	Практическое занятие		**2**	
	3	Изучение механизмов защиты СУБД MS ACCESS	2	
	Контрольные работы *(не предусмотрены)*			
	Внеаудиторная самостоятельная работа обучающихся		**2**	
	2	Подготовка сообщения на тему: «Схема идентификации Гиллоу - Куискуотера.»	2	
Тема 1.4.	**Содержание учебного материала**		**1**	
	1	Общие сведения. Совместное применение средств идентификации и аутентификации, встроенных в СУБД и в ОС.	1	ОК 01., ОК 02., ОК 04., ОК 05.,

Средства идентификации и аутентификации	Лабораторные работы *(не предусмотрены)*		-	ОК 09., ПК 1.4., ПК 11.5., ПК 11.6.
	Практическое занятие		**2**	
	4	Идентификация и аутентификация объектов сети.	2	
	Контрольные работы *(не предусмотрены)*		-	
	Внеаудиторная самостоятельная работа обучающихся *(не предусмотрены)*		-	
Тема 1.5. Средства управления	**Содержание учебного материала**		**1**	ОК 01., ОК 02., ОК 04., ОК 05., ОК 09., ПК 1.4., ПК 11.5., ПК 11.6.
	1	Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Виды привилегий: привилегии безопасности и доступа. Использование ролей и привилегий пользователей. Соотношение прав доступа, определяемых ОС и СУБД.	1	
доступом		Использование представлений для обеспечения конфиденциальности информации в СУБД. Средства реализации мандатной политики безопасности в СУБД.		
	Лабораторные работы *(не предусмотрены)*		-	
	Практическое занятие		**2**	
	5	Использование ролей и привилегий пользователей.	2	
	Контрольные работы *(не предусмотрены)*		-	
	Внеаудиторная самостоятельная работа обучающихся *(не предусмотрены)*		-	
Тема 1.6. Целостность БД и способы ее обеспечения	**Содержание учебного материала**		**1**	ОК 01., ОК 02., ОК 04., ОК 05., ОК 09., ПК 1.4., ПК 11.5., ПК 11.6.
	1	Основные виды и причины возникновения угроз целостности. Способы противодействия. Цели использования триггеров. Способы задания, моменты выполнения. Декларативная и процедурная ссылочные целостности. Внешний ключ. Способы поддержания ссылочной целостности.	1	
	Лабораторные работы *(не предусмотрены)*		-	
	Практические занятия *(не предусмотрены)*		-	
	Контрольные работы *(не предусмотрены)*		-	
	Внеаудиторная самостоятельная работа обучающихся		**2**	

	3	Сообщение/презентация на тему: «Три вида возможных нарушений информационной системы.»	2	
Тема 1.7. Классификация угроз конфиденциальност и СУБД	**Содержание учебного материала**		**1**	ОК 01., ОК 02., ОК 04., ОК 05., ОК 09., ПК 1.4., ПК 11.5., ПК 11.6.
	1	причины, виды, основные методы нарушения конфиденциальности. Типы утечки конфиденциальной информации из СУБД, частичное разглашение. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов. Методы противодействия. Особенности применения криптографических методов.	1	
	Лабораторные работы *(не предусмотрены)*		-	
	Практическое занятие		**2**	
	6	Получение несанкционированного доступа к конфиденциальной информации путем логических выводов.	2	
	Контрольные работы *(не предусмотрены)*		-	
	Внеаудиторная самостоятельная работа обучающихся *(не предусмотрены)*		-	
Тема 1.8.	**Содержание учебного материала**		**2**	ОК 1,

Аудит и подотчетность	1	Подотчетность действий пользователя и аудит связанных с безопасностью событий. Регистрация действий пользователя. Управление набором регистрируемых событий. Анализ регистрационной информации.	2	ОК 01., ОК 02., ОК 04., ОК 05., ОК 09., ПК 1.4., ПК 11.5., ПК 11.6.
	Лабораторные работы *(не предусмотрены)*			
	Практическое занятие.		**4**	
	7	Регистрация событий (аудит).	2	
	8	Настройка параметров регистрации и аудита операционной системы	2	
	Контрольные работы *(не предусмотрены)*		-	
	Внеаудиторная самостоятельная работа обучающихся *(не предусмотрены)*		-	
	Содержание учебного материала		**2**	

Тема 1.9. Транзакции и блокировки	1	Транзакции как средство изолированности пользователей. Сериализация транзакций. Методы сериализации транзакций. Режимы блокировок. Правила согласования блокировок. Двухфазный протокол синхронизационных блокировок. Тупиковые ситуации, их распознавание и разрушение.	2	ОК 01., ОК 02., ОК 04., ОК 05., ОК 09., ПК 1.4., ПК 11.5., ПК 11.6.
	Лабораторные работы *(не предусмотрены)*		-	
	Практическое занятие		**2**	
	9	Применение транзакций как средства изолированности пользователей. Режимы блокировок.	2	
	Контрольные работы *(не предусмотрены)*		-	
	Внеаудиторная самостоятельная работа обучающихся		**2**	
	4	Написание сообщения на тему: «Целостность кода приложения. SQL-инъекции. Динамическое выполнение кода SQL и PL/SQL. Категории атак SQL-инъекцией. Методы SQL-инъекций».	2	
Тема 1.10. Стандартные методы защиты объектов базы данных	**Содержание учебного материала**		**2**	ОК 01., ОК 02., ОК 04., ОК 05., ОК 09., ПК 1.4., ПК 11.5., ПК 11.6.
	1	Основные понятия и определения. Понятие криптографического протокола. Методы аутентификации, использующие пароли и PIN-коды: на основе многоразовых паролей, на основе одноразовых паролей, на основе сертификатов. Строгая аутентификация, основанная: на симметричных алгоритмах, на асимметричных алгоритмах, на однонаправленных хеш-функциях. Биометрическая аутентификация пользователя.	2	
	Лабораторные работы *(не предусмотрены)*		-	
	Практическое занятие		**2**	
	10	Методы криптографии	2	
	Контрольные работы *(не предусмотрены)*		-	
	Внеаудиторная самостоятельная работа обучающихся		**2**	
	5	Сообщение/презентация по теме «Криптоанализ», «Электронно-цифровая подпись»	2	
Дифференцированный зачет			**2**	

Всего:	**46**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение Лаборатория программирования и баз данных. Оборудование учебного кабинета:

1. комплекты специализированной учебной мебели,
2. маркерная доска,

Технические средства обучения:

3. проектор,
4. экран,
5. автоматизированные рабочие места по количеству обучающихся (не менее 12-15 АРМ) (Core i5, оперативная память объемом 8GB, монитор 23.8", мышь, клавиатура) с выходом в сеть «Интернет» и доступом в электронную информационно-образовательную среду, , МФУ формата А4.
6. Лицензионное программное обеспечение общего и профессионального назначения, в т.ч. ОС Windows, MS Office, 7-Zip , Adobe Acrobat Reader, Comodo Internet Security, Bloodshed Dev-C++, Apache NetBeans, MySQL for Windows, Android Studio
7. Доступы с компьютеров каб. 405 к серверу в каб. 110 (8-х ядерный процессор с частотой 3 ГГц, оперативная память объемом 16 Гб, жесткие диски общим объемом не менее 1 Тб, программное обеспечение: WindowsServer).

3.2. Информационное обеспечение обучения

Перечень учебных изданий, дополнительной литературы, Интернет-источников

Основные источники:

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 9785-534-10671-8. - URL: https://urait.ru/bcode/475889

Дополнительные источники:

2. 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. - 161 с. - (Профессиональное образование). - ISBN 978-5-534-13948-8. - URL: https: //urait. ru/bcode/475890

3. 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

4. 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

5. 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

6. 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 978-5-53414328-7 (Издательство Юрайт). - ISBN 978-5-8154-0518-9 (КемГИК). - URL: https://urait.ru/bcode/477568

7. Гендина, Н. И. Информационная культура личности в 2 ч. Часть 2: 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. - 308 с. - (Высшее образование). - ISBN 978-5-53414419-2 (Издательство Юрайт). - ISBN 978-5-8154-0518-9 (КемГИК). - URL: https: //urait. ru/bcode/477569

Интернет-источники

1. http://www.edu.ru - Российское образование - Федеральный портал;
2. http://www.wikipedia.ord - информационный портал википедиа;
3. http: //www.topreferat. znate. ru - все для студента;

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

Результаты обучения	Коды формируемых профессиональных и общих компетенций	Формы и методы оценки
Перечень умений, осваиваемых в рамках дисциплины: - 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. - 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.	ОК 1, ОК 2 ОК 4, ОК 5, ОК 9, ПК 1.4, ПК 4.5, ПК 4.6	Опрос (устный/письменный) Тестирование. Оценка внеаудиторной самостоятельной работы. Подготовка и выступление с докладом/сообщением. Наблюдение за выполнением практического задания. (деятельностью студента) Оценка выполнения практического задания (работы). Решение ситуационной задачи.