Комитет образования, науки и молодежной политики Волгоградской области
**ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ «ВОЛГОГРАДСКИЙ СОЦИАЛЬНО-ПЕДАГОГИЧЕСКИЙ КОЛЛЕДЖ»**
(ГАПОУ «ВСПК»)

**УТВЕРЖДАЮ**
Директор ГАПОУ «ВСПК»
_____/А.С. Калинин /
«__» _____2020г.

ГАПОУ «ВСПК»

# ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

## Информационная безопасность

**Объем**: 72 часа

**Форма обучения**: очная, с применением ДОТ

г. Волгоград, 2020

Автор программы: Машихина Т.П,. к.п.н.,доцент,
Бекингалиева А.Ж., преподаватель информатики ГАПОУ «ВСПК».

Программа рассмотрена на заседании кафедры информационных технологий обучения

Протокол заседания № 3 от « 1 » октября 2020 г.

Заведующий кафедрой информационных технологий обучения

_____к.п.н., доцент, Машихина Т.П.
*Фамилия И.О., подпись*

Программа рассмотрена на заседании научно-методического совета ГАПОУ «ВСПК»

Протокол НМС № 96 от «1 » октября 2020 г.

Заместитель директора по учебно-воспитательной работе

_____Герасименко С.В.
*Фамилия И.О., подпись*

**Оглавление**

## 1.Паспорт образовательной программы

### 1.1. Область применения программы

Программа повышения квалификации педагогических работников реализуется на базе мастерской по компетенции «Программное решение для бизнеса». с применением оборудования мастерской и оснащения рабочих мест в соответствии с инфраструктурным листом WorldSkills Russia.

Содержание настоящей программы направлено на совершенствование профессионального уровня слушателей в рамках имеющейся квалификации, в том числе на овладение ими современными компьютерными технологиями для защиты данных.

### 1.2. Цели и задачи программы – требования к результатам освоения программы

**Цель программы** – дать общие представления о безопасности в информационном обществе и на этой основе сформировать понимание технологий информационной безопасности и умения применять правила кибербезопасности во всех сферах деятельности.

**Задачи программы:**

- Формирование необходимого минимума специальных теоретических знаний и практических навыков по следующим аспектам: основные положения и история развития информационной безопасности, методики построения моделей гроз и злоумышленника, методология построения систем защищенных ИС, методы защиты разных видов информации, проектирование политик и моделей безопасности предприятия;
- Формирование методологических основ в области информационной безопасности;
- Формирование навыков работы с методами оценки рисков информационной безопасности (ИБ) предприятия.

**В результате освоения программы слушатели должны:**

**знать:**

- основные положения информационной безопасности российской федерации;
- уязвимости, воздействия нарушителя и угрозы информационной безопасности глобальных сетей передачи данных (вопросы методологии);
- модель воздействий нарушителя на информационную сферу ГСПД;
- угрозы информационной безопасности ГСПД;
- системы безопасности и способов создания учетных записей, групп и ролей SQL Server.

**уметь:**

- создавать учетные записи, группы и роли SQL Server;
- исследовать и выделить наиболее значимые показатели качества (ПК) для заданного объекта;
- Определять перечень актуальных угроз;
- Настраивать разрешения на доступ к файлам в операционных системах семейства Windows компьютера, периферийного и мультимедийного оборудования.

### 1.3. Количество часов на освоение программы

**Объем учебной нагрузки** по освоению программы рассчитан на 72 часа, обязательной аудиторной учебной нагрузки обучающегося, в том числе 40 часов с применением ДОТ.

**2. Результаты освоения программы.**

**Целевая аудитория:** педагогические работники.

**Форма организации образовательного процесса:** очная с элементами дистанционных технологий: часы лекций и практики.

**Формы работы**: интерактивные лекции с использованием материально-технической базы мастерской по компетенции «Программные решения для бизнеса», практические занятия, семинары, мастер-классы, круглые столы, экспресс-опросы, индивидуальные и групповые проекты и др. В ходе занятий слушатели получают необходимую теоретическую информацию, участвуют в дискуссиях, выполняют учебно-практические задания.

В рамках итоговой аттестации слушатели проходят итоговое тестирование..

**Планируемые результаты обучения.**

В результате обучения слушатель, успешно освоивший программу, научится:

- владеть навыками работы с компьютером, технологией работы с программными комплексами в соответствии с особенностями профессиональных запросов слушателей;
- владеть навыками защиты данных при помощи создания резервных копий и восстановления данных;
- владеть навыками защиты информации в базе данных Access от несанкционированного доступа;
- владеть приемами работы с защищенными базами данных из программ VBA;
- владеть навыками настройки разрешений на доступ к файлам в операционных системах семейства Windows.

## 3. Структура и содержание программы

### 3.1. Тематическое планирование программы

| Название раздела | Всего часов | Лекционные занятия | Практические занятия | В том числе с ДОТ | |
|---|---|---|---|---|---|
| | | | | Лекции | Практика |
| Тема 1. Основные Положения Информационной Безопасности Российской Федерации | 10 | 8 | 2 | | 1 |
| Тема 2 Уязвимости, воздействия нарушителя и угрозы информационной безопасности глобальных сетей передачи данных (Вопросы Методологии) | 16 | 6 | 10 | 4 | 6 |
| Тема 3. Уязвимость ГСПД | 14 | 6 | 8 | 4 | 5 |
| Тема 4. Модель Воздействий Нарушителя На Информационную Сферу ГСПД | 16 | 6 | 10 | 4 | 6 |
| Тема 5. Угрозы Информационной Безопасности ГСПД | 16 | 6 | 10 | 4 | 6 |
| **Всего** | **72** | **32** | **40** | **16** | **24** |

### 3.2. Содержание программы

**Тема 1. Основные Положения Информационной Безопасности Российской Федерации**

**Содержание:**

Модели безопасности, политика безопасности, теоретические основы информационной безопасности.

**Оборудование:** ПК, проектор, интерактивная доска.

Дидактический материал: материалы лекций, презентации.

**Тема 2 Уязвимости, воздействия нарушителя и угрозы информационной безопасности глобальных сетей передачи данных (Вопросы Методологии).**

**Содержание:**

Информационные системы, проектирование информационных систем, экспертная оценка угроз, система безопасности SQL Server 2008.

**Оборудование:** ПК, интерактивная доска, проектор.

Дидактический материал: лекционный материал, лабораторные работы.

**Тема 3. Уязвимость ГСПД.**

**Содержание:**

Постановка задачи обеспечения информационной безопасности баз данных.

Экспертная оценка качества.

Экспертное оценивание в управлении информационной безопасность.

Классы безопасности АС.

**Оборудование:** ПК, интерактивная доска, проектор.

Дидактический материал: лабораторные работы, презентации.

**Тема 4. Модель Воздействий Нарушителя На Информационную Сферу ГСПД.**

**Содержание:**

Угрозы информационной безопасности БД.

Атаки, специфические для БД.

Создание резервных копий файлов для баз данных и проектов Access.

Понятие и состав модели нарушителя.

Содержательная (описательная) модель нарушителя.

**Оборудование:** ПК, проектор, интерактивная доска.

Дидактический материал: лекционный материал, лабораторные работы.

**Тема 5. Угрозы Информационной Безопасности ГСПД.**

**Содержание:**

Методы дискреционного разграничения доступа.

Анализ методов аутентификации участников взаимодействия в процессе обработки БД.

Работы с защищенными БД из программ VBA.

Управление доступом к файлам на NTFS.

KASPERSKY SECURITY CENTER.

Сценарии воздействия нарушителя на основе графов.

Сценарии воздействия нарушителя на основе деревьев.

Модель злоумышленных воздействий с использованием сетей Петри

**Оборудование:** ПК, проектор, интерактивная доска.

Дидактический материал: лекции, лабораторные работы, презентации.

.

## 4. Условия реализации программы повышения квалификации

### 4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы повышения квалификации предполагает наличие рабочих мест, оснащенных в соответствии с инфраструктурным листом WorldSkills Russia по компетенции «Программные решения для бизнеса».

**Технические средства обучения**

- рабочие станции слушателей и преподавателя, оборудованные современными персональными компьютерами и объединенными в локальную компьютерную сеть с возможностью доступа к учебному серверу и выходом в Интернет;
- мультимедийный проектор;
- интерактивная доска (интерактивная панель) на несколько касаний;
- многофункциональные устройства: чёрно-белое и цветное.

**Информационное обеспечение обучения предусматривает наличие следующего программного и методического обеспечения**: MS Windows, MS Office 2019 pro, SQL Server

### 4.2. Общие требования к организации образовательного процесса

Программа повышения квалификации ориентирована на педагогических работников, владеющих начальными навыками работы с ПК.

**Наполняемость учебной группы:** по числу автоматизированных рабочих мест мастерской – не более 10 человек.

Продолжительность учебного часа теоретических и практических занятий в аудиторном формате и дистанционном режиме составляет 1 академический час (45 минут) на группу.

**Требования к педагогическим кадрам:**

Преподаватели, реализующие программу повышения квалификации, должны удовлетворять квалификационным требованиям, указанным в квалификационных справочниках по соответствующим должностям и

профессиональном стандарте педагога.

### 4.3. Учебно-методическое обеспечение

**Список источников:**


1. Инструментальный контроль и защита информации [Электронный ресурс]: учебное пособие/ Н.А. Свинарев [и др.].— Электрон. Текстовые данные.— Воронеж: Воронежский государственный университет инженерных технологий, 2013.— 192 с.— Режим доступа: http://www.iprbookshop.ru/47422.html.
2. Калмыков И.А. Криптографические методы защиты информации [Электронный ресурс]: лабораторный практикум/ Калмыков И.А., Науменко Д.О., Гиш Т.А.— Электрон. Текстовые данные.— Ставрополь: СевероКавказский федеральный университет, 2015.— 109 с.— Режим доступа: http://www.iprbookshop.ru/63099.html.
3. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Серия : Университеты России). — ISBN 978-5-534-00258-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/434171 (дата обращения: 06.05.2019)
4. Основы информационной безопасности : опорный конспект / Е.А. Рыбакова. - СПб.: Изд-во СЗТУ, 2016. - 49 с. 2. Васильев В.И. Интеллектуальные системы защиты информации [Электронный ресурс]: учебное пособие/ Васильев В.И.— Электрон. Текстовые данные.— М.: Машиностроение, 2013.— 172 с.— Режим доступа: http://www.iprbookshop.ru/18519.html
5. Пашинцев В.П. Нестандартные методы защиты информации [Электронный ресурс]: лабораторный практикум/ Пашинцев В.П., Ляхов А.В.— Электрон. Текстовые данные.— Ставрополь: Северо-Кавказский федеральный университет, 2016.— 196 с.— Режим доступа: