

Составители (разработчики) программы:
Внукова Наталья Владимировна, преподаватель ОГАПОУ «Белгородский
индустриальный колледж»

ОГЛАВЛЕНИЕ

№ п/п	Наименование документа	стр.
1.	Пояснительная записка	4
2.	Содержание программы	8
2.1.	Учебный план программы	8
2.2.	Учебно-тематический план программы	9
2.3.	Календарный учебный график	11
2.4.	Рабочая программа	12
3.	Формы аттестации	15
3.1.	Оценочные материалы	15
4.	Организационно-педагогические условия	16
4.1.	Материально-техническое обеспечение программы	16
4.2.	Учебно-информационное обеспечение программы	16
4.3.	Кадровое обеспечение программы	16

1. Пояснительная записка

Дополнительная профессиональная программа повышения квалификации «Современные технологии организации информационной безопасности (подготовка кадров по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»)» (40 часов) разработана с учётом требований и положений:

– Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

– Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам (утв. приказом Министерства образования и науки РФ от 1 июля 2013 г. № 499);

– Порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности (утв. приказом Министерства образования и науки РФ от 05 декабря 2013 г. № 1310);

– Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (утв. приказом Министерства образования и науки РФ от 9 декабря 2016 г. № 1551);

– Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.01 Организация и технология защиты информации (утв. приказом Министерства образования и науки РФ от 28.07.2014 N 805 (ред. от 13.07.2021));

– Спецификацией стандарта компетенции «Корпоративная защита от внутренних угроз информационной безопасности» (WorldSkills Standards Specifications);

– Приказом Министерства образования и науки Российской Федерации от 02.07.2013 № 513 «Об утверждении Перечня профессий рабочих, должностей служащих, по которым осуществляется профессиональное обучение».

Реализация Программы предусмотрена на базе ОГАПОУ «Белгородский индустриальный колледж» на основе Устава.

Организация-разработчик: ОГАПОУ «Белгородский индустриальный колледж».

Дополнительная профессиональная программа повышения квалификации направлена на совершенствование и (или) получение новой компетенции, необходимой для профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации, с учетом спецификации стандарта Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»

Цели программы:

- ознакомление преподавателей с современными технологиями в профессиональной сфере деятельности и стандартами Ворлдскиллс по соответствующей компетенции;

- создание условий по изучению требований к уровню подготовки выпускников на основе стандартов Ворлдскиллс России по компетенции «Корпоративная защита от внутренних угроз информационной безопасности».

Задачи программы:

- ознакомление с содержанием, структурой движения WorldSkills в России;
- изучение нормативной базы проведения демонстрационных экзаменов по методике WorldSkills;
- ознакомление с порядком организации и проведения демонстрационного экзамена, включая требования к процедурам и участникам, содержанием и структурой компетенции «Корпоративная защита от внутренних угроз информационной безопасности»;
- освоение технологии выполнения практических заданий демонстрационного экзамена с применением методики Worldskills Russia по компетенции «Корпоративная защита от внутренних угроз информационной безопасности».

Категория слушателей, на обучение которых рассчитана программа дополнительного профессионального образования (далее – программа): преподаватели (мастера производственного обучения) профессиональных образовательных организаций, реализующих программы среднего профессионального образования.

Полученные в ходе повышения квалификации профессиональные компетенции, умения и знания предназначены для применения при планировании реализации основных образовательных программ, программ профессионального обучения и дополнительного профессионального образования, решающих задачи подготовки специалистов среднего звена.

Слушатель, приступающий к освоению программы, должен владеть основами работы на персональном компьютере, уметь работать с программным обеспечением Microsoft Office или его аналогами.

Обучение по программе ведется на русском языке.

Трудоемкость обучения: нормативная трудоемкость обучения по данной программе составляет 40 академических часа.

Форма обучения: очная.

1.1. Планируемые результаты освоения программы:

знать:

- стандарт компетенции «Корпоративная защита от внутренних угроз информационной безопасности» Ворлдскиллс Россия;
- методику реализации основной профессиональной образовательной программы (программы профессионального обучения) и отдельных профессиональных модулей с учетом стандарта компетенции «Корпоративная защита от внутренних угроз информационной безопасности» Ворлдскиллс Россия;
- структуру движения WorldSkills в России; нормативную базу проведения

демонстрационных экзаменов по методике WorldSkills;

- порядок организации и проведения демонстрационного экзамена, включая требования к процедурам и участникам, содержанию и структуре;

- технологию организации самообразования педагогов, технологию выполнения практических заданий демонстрационного экзамена с применением методики Worldskills Russia;

- практику и методику оценивания промежуточных и итоговых результатов обучения, организации и проведения демонстрационного экзамена по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» Ворлдскиллс Россия (примеры модульных заданий, организацию рабочего места, требования к технике безопасности, критерии и процедуру оценивания результатов);

- требования к материально-техническому обеспечению учебного процесса по основной профессиональной образовательной программе (программе профессионального обучения) с учетом соответствующего стандарта компетенции «Корпоративная защита от внутренних угроз информационной безопасности» Ворлдскиллс Россия.

уметь:

- внедрять современные педагогические технологии в рабочий процесс;
- организовывать и проводить демонстрационный экзамен с учетом требований к процедурам, участникам, содержанию и структуре компетенций;

- выполнять практические задания демонстрационного экзамена с применением методики Worldskills Russia по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»;

- организовывать обучение студентов и подготовку к сдаче демонстрационного экзамена по стандартам Ворлдскиллс Россия по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» в рамках государственной итоговой аттестации;

- проводить оценку промежуточных и итоговых результатов обучения студентов, оценку профессиональной компетентности студентов в ходе демонстрационного экзамена по стандартам Ворлдскиллс Россия по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»;

- организовывать разбор результатов, достигнутых студентами на демонстрационном экзамене по стандартам Ворлдскиллс Россия по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» и соответствующую актуализацию программ и методик обучения в целях достижения студентами высоких профессиональных результатов;

- использовать формы и методы обучения, в том числе, выходящие за рамки учебных занятий; объективно оценивать знания обучающихся на основе тестирования и других методов контроля.

владеть:

- различными педагогическими приемами, средствами, методами и технологиями, технологией выполнения практических заданий

демонстрационного экзамена с применением методики Worldskills;

- методикой проведения учебных занятий и организации самостоятельной работы обучающихся по учебным предметам, курсам, дисциплинам (модулям) образовательной программы с применением электронного обучения и дистанционных образовательных технологий; технологиями текущего контроля, оценки динамики подготовленности и мотивации обучающихся в процессе изучения учебного предмета, курса, дисциплины (модуля);

- различными педагогическими приемами, средствами, методами и технологиями;

- базовыми психолого-педагогическими умениями, не зависящими от специализации.

обладать:

профессиональными компетенциями, включающими в себя способность:

- создавать обучающую среду для полноценного обучения профессии/специальности;

- владеть технологией выполнения практических заданий демонстрационного экзамена с применением методики Worldskills Russia по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»;

- самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, расширять и углублять научное мировоззрение;

- совершенствовать и развивать свой интеллектуальный и общекультурный уровень;

- организация учебной деятельности обучающихся по освоению учебных предметов, курсов, дисциплин (модулей) программ профессионального обучения, СПО и (или) ДПП (ПК-1);

- педагогического контроля и оценки освоения образовательной программы профессионального обучения, СПО и (или) ДПП в процессе промежуточной и итоговой аттестации (ПК-2);

- разработки программно-методического обеспечения учебных предметов, курсов, дисциплин (модулей) программ профессионального обучения, СПО и(или) ДПП (ПК-3).

2. Содержание программы

2.1. Учебный план дополнительной профессиональной программы повышения квалификации «Современные технологии организации информационной безопасности (подготовка кадров по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»)»

Категория слушателей – административные и педагогические работники профессиональных образовательных организаций.

Срок обучения – 40 часов.

Форма обучения – очная.

№ п/п	Наименование дисциплин, модулей	Всего, ак.час.	В том числе:			
			Лекции	Практические занятия	Самостоятельная работа	Форма контроля
1	2	3	4	5	6	7
1.	Модуль 1. Стандарты Ворлдскиллс и спецификация стандартов Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности». Разделы спецификации	4	4			Собеседование
2.	Модуль 2. Современные технологии в профессиональной сфере. Основы защиты информации от внутренних угроз информационной безопасности	4	4			Собеседование
3.	Модуль 3. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	8	2	6		Практическое задание
4.	Модуль 4. Технологии агентского мониторинга	6	2	4		Практическое задание
5.	Модуль 5. Разработка политик безопасности, анализ выявленных инцидентов	6	2	4		Практическое задание

6.	Модуль 6. Современные технологии VPN. Система защиты информации VipNET	8	2	6		Практическое задание
Итоговая аттестация		4				Практическое задание в форме демонстрационного экзамена
Итого		40	16	24		

2.2. Учебно-тематический план дополнительной профессиональной программы повышения квалификации «Современные технологии организации информационной безопасности (подготовка кадров по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»)»

Категория слушателей – административные и педагогические работники профессиональных образовательных организаций.

Срок обучения – 40 часов.

Форма обучения – очная.

№ п/п	Наименование дисциплин, модулей	Всего, ак.час.	В том числе:			
			Лекции	Практические занятия	Самостоятельная работа	Форма контроля
1	2	3	4	5	6	7
1.	Модуль 1. Стандарты Ворлдскиллс и спецификация стандартов Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности». Разделы спецификации	4	4			Собеседование
1.1.	Тема 1. Движение WorldSkills Russia. Место движения в развитии системы профессионального образования	2	2			
1.2.	Тема 2. Стандарты и спецификация стандартов WorldSkills Russia по компетенции	2	2			

2.	Модуль 2. Современные технологии в профессиональной сфере. Основы защиты информации от внутренних угроз информационной безопасности	4	4			Собеседование
2.1	Тема 1. Основы защиты корпоративной информации	2	2			
2.2	Тема 2. Защита информации от внутренних угроз информационной безопасности. Выявление утечек с использованием технологии Data Leakage Prevention (DLP)	2	2			
3.	Модуль 3. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз	8	2	6		Практическое задание
3.1	Тема 1. Установка DLP IWTM в виртуальном окружении	6	2	4		
3.2	Тема 2. Конфигурирование DLP IWTM	2		2		
4.	Модуль 4. Технологии агентского мониторинга	6	2	4		Практическое задание
4.1	Тема 1. Назначение агентского мониторинга. Установка и настройка агентского мониторинга	4	2	2		
4.2	Тема 2. Политики агентского мониторинга, особенности их настройки. Создание и проверка политик	2		2		
5.	Модуль 5. Разработка политик безопасности,	6	2	4		Практическое задание

	анализ выявленных инцидентов					
5.1	Тема 1. Разработка и тестирование политик в системе DLP IWTM	6	2	4		
6.	Модуль 6. Современные технологии VPN. Система защиты информации VipNET	8	2	6		Практическое задание
6.1	Тема 1. Введение в технологию VipNET	2	2			
6.2	Тема 2. Компоненты управления сети VipNET	2		2		
6.3	Тема 3. Клиентские продукты VipNET	2		2		
6.4	Тема 4. Серверные продукты VipNET	2		2		
	Итоговая аттестация	4				Практическое задание в форме демонстрационного экзамена
	Итого	40	16	24		

2.3. Календарный учебный график

График обучения	Ауд. часов в день	Дней в неделю	Общая продолжительность программы, месяцев (дней, недель)
Форма обучения			
очная	8	5	40 часов, 5 дней, 1 неделя

2.4. Рабочая программа дополнительной профессиональной программы повышения квалификации «Современные технологии организации информационной безопасности (подготовка кадров по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»)»

№ п/п	Наименование темы	Содержание обучения (по темам в дидактических единицах), наименование и тематика лабораторных работ, практических занятий (семинаров), самостоятельной работы, используемых образовательных технологий и рекомендуемой литературы
1.	2.	3.
Модуль 1. Стандарты Ворлдскиллс и спецификация стандартов Ворлдскиллс по компетенции «Корпоративная защита от внутренних угроз информационной безопасности». Разделы спецификации		
1.	Тема 1. Движение WorldSkills Russia. Место движения в развитии системы профессионального образования	Лекция. История, современное состояние и перспективы движения WorldSkills International (WSI) и WorldSkills Russia («Молодые профессионалы») (2 часа)
2.	Тема 2. Стандарты и спецификация стандартов WorldSkills Russia по компетенции	Лекция. Актуальное техническое описание по компетенции. Спецификация стандарта WorldSkills Russia по компетенции «Корпоративная защита от внутренних угроз информационной безопасности» (2 часа)
Модуль 2. Современные технологии в профессиональной сфере. Основы защиты информации от внутренних угроз информационной безопасности		
1.	Тема 1. Основы защиты корпоративной информации	Лекция. Ключевые алгоритмы и системы. Основные понятия. Безопасность информационных систем. Угрозы информационной безопасности (2 часа)
2.	Тема 2. Защита информации от внутренних угроз информационной безопасности. Выявление утечек с использованием технологии Data Leakage Prevention (DLP)	Лекция. Теория и практика применения DLP-систем (2 часа)
Модуль 3. Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз		

1.	Тема 1. Установка DLP IWTM в виртуальном окружении	<p>Лекция.</p> <p>Сетевое окружение; сетевые протоколы; разнообразие операционных систем, их возможности с точки зрения использования пользователями и для развёртывания компонент систем защиты от внутренних угроз; этапы установки системы корпоративной защиты от внутренних угроз; технологии программной и аппаратной виртуализации; особенности работы основных гипервизоров (мониторов виртуальных машин), таких как VirtualBox, VMWare Workstation (2 часа)</p> <p>Практическое занятие.</p> <p>Создание лабораторного стенда в виртуальном окружении (4 часа)</p>
2.	Тема 2. Конфигурирование DLP IWTM	<p>Практическое занятие.</p> <p>Настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом (2 часа)</p>
Модуль 4. Технологии агентского мониторинга		
1.	Тема 1. Назначение агентского мониторинга. Установка и настройка агентского мониторинга	<p>Лекция.</p> <p>Функции агентского мониторинга; общие настройки системы агентского мониторинга; соединение с LDAP-сервером и синхронизация с Active Directory; политики агентского мониторинга, особенности их настройки; особенности настроек событий агентского мониторинга; механизмы диагностики агента, подходы к защите агента (2 часа)</p> <p>Практическое занятие.</p> <p>Установка и настройка агентского мониторинга (2 часа)</p>
2.	Тема 2. Политики агентского мониторинга, особенности их настройки. Создание и проверка политик	<p>Практическое занятие.</p> <p>Создание политик защиты на агентах (2 часа)</p>
Модуль 5. Разработка политик безопасности, анализ выявленных инцидентов		
1.	Тема 1. Разработка и тестирование политик в системе DLP IWTM	<p>Лекция.</p> <p>Технологии работы с политиками информационной безопасности; общие принципы при работе интерфейсом системы защиты корпоративной информации; объекты защиты, персоны; ключевые технологии анализа трафика (2 часа)</p> <p>Практическое занятие.</p> <p>Создать в системе максимально полный набор политик безопасности, перекрывающий все возможные каналы передачи данных и возможные инциденты (4 часа)</p>
Модуль 6. Современные технологии VPN. Система защиты информации VipNET		

1.	Тема 1. Введение в технологию VipNET	Лекция. Структура виртуальной защищенной сети. Назначение виртуальной защищенной сети. Особенности построения VPN-сетей. Основные типы классификаций VPN-сетей; Нормативно-правовые документы, требования законодательства и регулирующих органов РФ в области электронной подписи, удостоверяющих центров, СКЗИ, МЭ (2 час)
2.	Тема 2. Компоненты управления сети VipNET	Практическое занятие. Технологии построения виртуальных защищенных сетей на основе программных и программно-аппаратных решений; ключевые компоненты VPN-сетей (2 часа)
3.	Тема 3. Клиентские продукты VipNET	Практическое занятие. Особенности VPN-сети и механизмы их управления (2 часа)
4.	Тема 4. Серверные продукты VipNET	Практическое занятие. Назначение и роль доверенного удостоверяющего центра в системе ключевой инфраструктуры организации (2 часа)

3. Формы итоговой аттестации

По дополнительной профессиональной программе повышения квалификации «Современные технологии организации информационной безопасности (подготовка кадров по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»)» проводится контроль знаний слушателей: входной, текущей, итоговый контроль.

Текущий контроль проводится по каждой теме в виде собеседования и/или практического занятия с целью определения уровня самостоятельной работы слушателей по учебным материалам. Контроль текущих знаний проводится на занятиях в форме устного или письменного опроса, теста. Объектами текущего контроля при изучении дисциплин являются: посещение лекций; подготовка и качество выполнения практических работ.

Промежуточная аттестация слушателей данного курса повышения квалификации осуществляется в форме теста.

Промежуточная аттестация оценивается положительно оценками: «зачтено», либо отрицательно – «не зачтено».

Итоговая аттестация проводится в форме итоговой практической работы с элементами демонстрационного экзамена оценивается положительно оценками: «отлично», «хорошо», «удовлетворительно», либо отрицательно – «неудовлетворительно». Передача неудовлетворительной оценки допускается не более двух раз. Требования к уровню освоения программы владение знаниями учебных дисциплин в объеме не менее 75%.

3.1. Оценочные материалы

Итоговая аттестация слушателей

Для итоговой аттестации используется Комплект оценочной документации (КОД) № 1.1 по компетенции «Современные технологии организации информационной безопасности (подготовка кадров по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»)», размещенный в соответствующем разделе на электронном ресурсе esat.worldskills.ru. По результатам освоения программы дополнительного профессионального обучения выдается удостоверение о повышении квалификации.

4. Организационно-педагогические условия

4.1. Материально-техническое обеспечение программы

Реализация программы предполагает наличие материально-технической базы, соответствующей действующим санитарно-техническим нормам и обеспечивающим проведение всех видов подготовки слушателей, предусмотренных учебным планом. Материально-техническое обеспечение учебного процесса соответствует требованиям к современной организации образовательного процесса, включает наличие учебных аудиторий, мультимедийных проекторов, компьютеров.

Оборудование учебного кабинета:

1. Компьютерный класс и мультимедиа;
2. Мастерская «Анализ защищенности информационных систем от внешних угроз»;
3. Доступ к информационно-коммуникационной сети интернет.

Программное обеспечение:

- операционная система Windows (версия 2010 и выше);
- гипервизор VM Ware Workstation;
- операционная система MS Windows Server версии 2016 с поддержкой установки DLP системы и ПО для развертывания VPN, поддержка работы в режиме доменного контроллера;
- программное обеспечение для борьбы с внутренними утечками информации InfoWatch Traffic Monitor 6.10.24 (минимальный состав Infowatch Traffic Monitor, Infowatch Device Monitor, Crawler);
- программное обеспечение для защиты сетей связи в составе Учебно-методический комплекс «WorldSkills» сроком на 1 год в составе: ViPNet Administrator 4.x, ViPNet Coordinator Windows 4.x, ViPNet Coordinator Linux, ViPNet Client 4.x, Registration Point 4.x, ViPNet Publication Service 4.x, ViPNet Policy Manager 4.x, узел управления Policy Manager, ViPNet Coordinator HW-VA.

4.2. Учебно-информационное обеспечение программы

Основная литература:

1. Методика организации и проведения демонстрационного экзамена по стандартам Ворлдскиллс Россия, утвержденная приказом Союза «Ворлдскиллс Россия».
2. Комплект оценочной документации №1.1 по компетенции «Современные технологии организации информационной безопасности (подготовка кадров по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»)» (утвержден командой управления компетенций Союза «Ворлдскиллс Россия»).
3. Кодекс этики движения WorldSkills Russia.
4. Инструкция по охране труда и технике безопасности по компетенции «Корпоративная защита от внутренних угроз информационной безопасности»).

5. <https://worldskills.ru/o-nas/dvizhenie-worldskills/istoriya/>.

6. сайт Союза Ворлдскиллс Россия (<https://worldskills.ru>).

Дополнительная литература:

1. Компьютерные сети. 6-е изд. / Э. Таненбаум. – СПб.: Питер, 2016. – 992 с.: ил. – (Серия «Классика Computer Science»).

3. Компьютерные сети. Принципы, технологии, протоколы. 6-е изд./ В. Г. Олифер, Н. А. Олифер. – СПб.: Питер, 2020. – 958 с.: ил.

4.3. Кадровое обеспечение программы

Реализация программы должна обеспечиваться высококвалифицированными преподавателями, привлеченными специалистами, экспертами WS ведущих образовательных организаций и учреждений дополнительного профессионального образования, профессиональных образовательных организаций и иных организаций.