Бюджетное учреждение профессионального образования

Ханты–Мансийского автономного округа–Югры

«Нижневартовский социально–гуманитарный колледж»

БУ «Нижневартовский социально–гуманитарный колледж»

УТВЕРЖДАЮ

Директор

 БУ «Нижневартовский социально –

гуманитарный колледж»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Н. П. Коробова

«08» апреля 2022 г.

**ПРОГРАММА**

**повышения квалификации**

**«Информационная безопасность в образовательной организации»**

**Автор программы:** Окунцев Павел Владимирович – преподаватель БУ «Нижневартовского социально–гуманитарного колледжа» г. Нижневартовска.

**Категория слушателей:** работники образовательных учреждений.

**Форма обучения:** *заочная с применением дистанционных образовательных технологий и электронного обучения.*

**Программа одобрена на заседании** педагогического совета

БУ «Нижневартовский социально-гуманитарный колледж»

(протокол № 52 от 07 апреля 2022)

**Трудоемкость программы -** 72 часа

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Общий объём, час** | **Аудиторные занятия, час** | **Практические занятия, час** | **СРС (дистанционно), час** | **Форма итоговой аттестации, час** |
| 72 | 24 | 20 | 24 | Итоговое тестирование (2 часа) |

Нижневартовск, 2022

**ОГЛАВЛЕНИЕ**

[АННОТАЦИЯ 3](#_Toc59710903)

[ПОЯСНИТЕЛЬНАЯ ЗАПИСКА 4](#_Toc59710904)

[1. ЦЕЛЬ ПРОГРАММЫ. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ 5](#_Toc59710905)

[2. УЧЕБНЫЙ ПЛАН 6](#_Toc59710906)

[3. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК 8](#_Toc59710907)

[4. РАБОЧИЕ ПРОГРАММЫ МОДУЛЕЙ 9](#_Toc59710908)

[5. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ 11](#_Toc59710909)

[6. ФОРМЫ АТТЕСТАЦИИ 14](#_Toc59710910)

[7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И ИНЫЕ КОМПОНЕНТЫ 17](#_Toc59710911)

АННОТАЦИЯ

Программа повышения квалификации «Информационная безопасность в образовательной организации» (далее - Программа) разработана в рамках реализации мероприятия «Государственная поддержка профессиональных образовательных организаций в целях обеспечения соответствия их материально-технической базы современным требованиям в рамках федерального проекта «Молодые профессионалы» (повышение конкурентоспособности профессионального образования)» национального проекта «Образование» государственной программы Российской Федерации «Развитие образования».

Программа повышения квалификации составлена с учетом приказа Министерства образования и науки Российской Федерации от 1 июля 2013 г. № 499 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам», приказа Министерства труда и социальной защиты РФ от 5 октября 2015 г. № 684н «Об утверждении профессионального стандарта «Системный администратор информационно-коммуникационных систем».

Программа включает пояснительную записку, основные требования к уровню освоения содержания дисциплины, учебный и учебно-тематический план, содержание разделов программы по модулям с кратким содержанием тематики, организационно-педагогические условия реализации программы, формы аттестации и оценочные материалы для обучения слушателей по программе, рассчитанной на 72 учебных часа.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Предлагаемая программа повышения квалификации направлена на формирование знаний об информационной безопасности в образовательной организации; знаний информационно-правовых аспектов безопасности информационных ресурсов, основные проблемы информационного права, информационно-правовых отношений; принципы и способы охраны интеллектуальной собственности; ознакомление с методами профилактики Интернет-зависимости среди обучающихся, формирование педагогической компетентности в сфере информационной безопасности и др.

*Актуальность* разработки программы повышения квалификации состоит в том, что она позволяет совершенствовать компетенции, необходимые для профессиональной деятельности и повышения профессионального уровня, в рамках имеющейся у слушателя квалификации.

В результате прохождения программы повышения квалификации

обучающиеся должны усовершенствовать свои знания, умения и навыки, которые участвуют в качественном изменении или формировании новых компетенций в результате освоения слушателем программы.

Ожидаемый эффект реализации программы - владение методами и программными средствами обработки деловой информации, анализа деятельности и управления персоналом, способностью взаимодействовать со службами информационных технологий и эффективно использовать корпоративные информационные системы.

Нормативный срок освоения программы составляет 72 часа, в том числе: теоретическое обучение - 24 часа, практические занятия – 20 часов, самостоятельная работа - 24 часа, итоговое тестирование - 2 часа.

Форма обучения: заочная с применением дистанционных образовательных технологий.

1. ЦЕЛЬ ПРОГРАММЫ. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

**Цель программы**: совершенствование у слушателей профессиональных компетенций в области информационной безопасности при организации образовательного процесса.

Поставленная цель достигается решением следующих задач:

* ознакомиться с информационной безопасностью в образовательной организации;
* рассмотреть информационно-правовые аспекты безопасности информационных ресурсов, основные проблемы информационного права, информационно-правовых отношений;
* изучить принципы и способы охраны интеллектуальной собственности;
* ознакомиться с методами профилактики Интернет-зависимости среди обучающихся;
* сформировать педагогические компетентности в сфере информационной безопасности.

**ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ**

Программа направлена на совершенствование следующую общепрофессиональную компетенцию (далее – ОПК):

ОПК-10 Владение методами и программными средствами обработки деловой информации, анализа деятельности и управления персоналом, способностью взаимодействовать со службами информационных технологий и эффективно использовать корпоративные информационные системы.

|  |  |  |  |
| --- | --- | --- | --- |
| **Общепрофессиональные компетенции** | **Практический опыт** | **Умения** | **Знания** |
| Владение методами и программными средствами обработки деловой информации, анализа деятельности и управления персоналом, способностью взаимодействовать со службами информационных технологий и эффективно использовать корпоративные информационные системы. | Освоение функциональных возможностей и предпосылки эффективного использования различных типов технологических систем и способов обработки и хранения традиционных и электронных конфиденциальных документов | Принимать меры по обеспечению безопасности | Гражданское, административное, трудовое законодательство в части, касающейся регулирования деятельности образовательных учреждений |

2. УЧЕБНЫЙ ПЛАН

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Раздел, тема** | **Виды учебной работы, включая самостоятельную работу слушателей и трудоемкость (в часах)** | **Форма аттестации** |
| **Всего** | **Лекции** | **Практические занятия** | **Самостоятельная****работа** |
| **1** | **Модуль 1.** Информационная безопасность в ОО: исторические предпосылки, основные понятия и определения. | **17** | **6** | **4** | **6** | **1** |
| 1.1. | Исторические предпосылки информационной безопасности образовательной организации | 4 | 2 |  | 2 |  |
| 1.2. | Основные направления информационной безопасности | 6 | 2 | 2 | 2 |  |
| 1.3. | Потенциальные объемы работ по защите информации в образовательной организации | 6 | 2 | 2 | 2 |  |
| 1.4. | Тестирование по модулю 1. | 1 |  |  |  | **Тестирование** |
| **2.** | **Модуль 2.** Информационная безопасность компьютеров, локальной сети, сервисов и информационных систем. | **25** | **8** | **8** | **8** | **1** |
| 2.1. | Оснащение современной образовательной организации. | 6 | 2 | 2 | 2 |  |
| 2.2. | Задачи, решаемые компьютерной техникой образовательной организации | 6 | 2 | 2 | 2 |  |
| 2.3. | Информационная безопасность персональных данных. | 6 | 2 | 2 | 2 |  |
| 2.4. | Технические работы по защите информации. | 6 | 2 | 2 | 2 |  |
| 2.5. | Тестирование по модулю 2. | 1 |  |  |  | **Тестирование** |
| **3.** | **Модуль 3.** Организационные меры по защите информации: создание нормативных документов и регламентов | **11** | **4** | **6** | **4** | **1** |
| 3.1. | Организационные меры по защите информации. | 4 | 2 |  | 2 |  |
| 3.2. | Составление регламентов и нормативных документов по обеспечению информационной безопасности учреждения. | **6** | **2** | **2** | **2** |  |
| 3.3. | Тестирование по модулю 3. | 1 |  |  |  |  |
| **4.** | **Модуль 4.** Обучение учащихся правилам безопасной работы в сети: практический инструментарий. | 19 | 6 | 6 | 6 | **1** |
| 4.1. | Обеспечение информационной безопасности и безопасности детей в сети Интернет | 6 | 2 | 2 | 2 |  |
| 4.2 | Защита детей от доступа к негативной информации | 6 | 2 | 2 | 2 |  |
| 4.3 | Всероссийский интернет-урок "Безопасность детей в Интернете": принципы, методы и формы организации. | 6 | 2 | 2 | 2 |  |
| 4.4. | Тестирование по модулю 4. | 1 |  |  |  |  |
| **5.** | **Модуль 5.** Итоговая аттестация (тестирование) | **2** |  |  |  | **Итоговое тестирование** |
| 5.1. | **Итого** | **72** | **20** | **24** | **24** | **2** |

3. КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

Календарный учебный план составляется при сформированной группе с учетом уровня их подготовки.

Календарный учебный график отражает периоды теоретических занятий, практик, процедур промежуточной и итоговой аттестаций и т.д.

КАЛЕНДАРНЫЙ УЧЕБНЫЙ ГРАФИК

|  |  |  |
| --- | --- | --- |
| **Учебные недели** | 1 | 2 |
| **Учебные занятия (Т)** | T |  |
| **Практические занятия (ПЗ)** | ПЗ | ПЗ |
| **Выездные занятия (В)** | – | – |
| **Контроль****Промежуточная аттестация (ПА)** | ПА | ПА |
| **Итоговое тестирование (ИТ)** | – | ИА |

4. РАБОЧИЕ ПРОГРАММЫ МОДУЛЕЙ

**Рабочая программа модуля 1. Информационная безопасность в ОО: исторические предпосылки, основные понятия и определения.**

Количество часов: 17 ч., в т.ч. лекций - 6 ч., практическая работа – 4 ч., самостоятельная работа - 6 ч., тестирование по модулю – 1 ч

**Лекция (2 ч.) Исторические предпосылки информационной безопасности образовательной организации.**

Информатизация. Угрозы для информации. Средства защиты информации. Информационные технологии в целом. История развития информационных технологий. Защита информации в целом.

**Лекция (2 ч.) Основные направления информационной безопасности.**

Направления информационной безопасности. Правовая защита. Организационная защита. Инженерно-техническая защита. Физические средства защиты. Аппаратные средства защиты. Программные средства защиты. Криптографические средства защиты.

**Лекция (2 ч.) Потенциальные объемы работ по защите информации в образовательной организации.**

Информатизация образования. Процесс информатизации образования. Этапы информатизации образования. Аспекты образовательных средств ИТ. Единое информационное пространство школы

**Самостоятельная работа (2 ч.)**

Изучить следующие материалы: Концептуальная модель информационной безопасности. Доктрина информационной безопасности РФ.

**Самостоятельная работа (2 ч.)**

Изучить следующие материалы: Угрозы безопасности данных. Основы методологии построения защищенных информационных систем

**Самостоятельная работа (2 ч.)**

Изучить следующие материалы: Информационная безопасность в образовательной организации

**Рабочая программа модуля 2. Информационная безопасность компьютеров, локальной сети, сервисов и информационных систем.**

Количество часов: 25 ч., в т.ч. лекционных – 8 ч., практических – 8 ч., самостоятельная работа – 8 ч., тестирование по модулю – 1 ч

**Лекция (2 ч.) Оснащение современной образовательной организации.**

Формирование цифровой образовательной среды в образовательной организации. Цифровая образовательная среда образовательной организации (ЦОС ОО). Единое информационно-образовательное пространство (ЕИОП). Безопасное информационное пространство общеобразовательной школы.

**Лекция (2 ч.) Задачи, решаемые компьютерной техникой образовательной организации.**

Информационные и коммуникационные технологии (ИКТ)**.** Средства ИКТ в системе образования**.** Аппаратные средства. Программные средства.

**Лекция (2 ч.) Информационная безопасность персональных данных.**

Информационная безопасность**.** Персональные данные**.** Обзор требований по защите персональных данных**.** Оператор персональных данных**.** Обеспечение безопасности персональных данных при их обработке.Информационная система персональных данных**.** Создание системы защиты персональных данных**.** Проверки регуляторов по обеспечению информационной безопасности персональных данных.

**Лекция (2 ч.) Технические работы по защите информации.**

Система органов государственной власти и управления в сфере информатизации и информационной безопасности. Организация системы лицензирования в области ТЗИ. Методика подготовки и проведения процедуры лицензирования деятельности. Аттестация объектов информатизации по требованиям безопасности. Сертификация средств защиты информации. Обеспечение безопасности в сетях.

**Практическая работа (4 ч.)**

Оснащение современной образовательной организации. Анализ и расчёты по группам объектов и средств материально-технического обеспечения в образовательной организации по месту работы слушателя КПК.

**Практическая работа (4 ч.)**

Информационная безопасность персональных данных. Технические работы по защите информации. Несанкционированный доступ. Паролирование. Технические средства защиты от НСД.

**Самостоятельная работа (2 ч.)**

Изучить следующие материалы: Цели и направления внедрения компьютерных технологий в педагогическую деятельность. Использование современных информационных и коммуникационных технологий в учебном процессе

**Самостоятельная работа (2 ч.)**

Изучить следующие материалы: Вирусы и антивирусные средства. Защита информации в глобальных сетях.

**Самостоятельная работа (2 ч.)**

Изучить следующие материалы: Правовые основы организации защиты персональных данных. Персональные даты для детей 9-11 лет. Персональные даты для детей 12-14 лет

**Самостоятельная работа (2 ч.)**

Изучить следующие материалы: Обеспечение безопасности в сетях**.** Криптографические методы защиты.

**Рабочая программа модуля 3. Организационные меры по защите информации: создание нормативных документов и регламентов.**

Количество часов: 11 ч., в т.ч. лекционных – 4 ч., практических – 2 ч., самостоятельная работа – 4 ч., тестирование по модулю – 1 ч

**Лекция (2 ч.) Организационные меры по защите информации.**

Организационная защита. Организационные средства защиты ПЭВМ и информационных сетей. Организационно служба безопасности.

**Лекция (2 ч.) Составление регламентов и нормативных документов по обеспечению информационной безопасности учреждения.**

Локальные нормативные акты в сфере обеспечения информационной безопасности обучающихся. Нормативная база. Федеральная служба по техническому и экспортному контролю (ФСТЭК). Федеральный закон № 149 - Основные понятия. Федеральный закон № 152 - Основные понятия. Модель отношений субъектов информационных отношений.

**Практическая работа (2 ч.)**

Комплексная безопасность образовательной организации. Мероприятия по комплексной безопасности образовательной организации в современных условиях. Сформировать мероприятия по комплексной безопасности в образовательной организации по месту работы слушателя КПК.

**Самостоятельная работа (2 ч.)**

Изучить следующие материалы: Организационные меры обеспечения информационной безопасности компьютерных систем. Политика информационной безопасности организации.

**Самостоятельная работа (2 ч.)**

Изучить следующие материалы: Составление регламентов и нормативных документов.

**Рабочая программа модуля 4. Модуль 4. Обучение учащихся правилам безопасной работы в сети: практический инструментарий.**

Количество часов: 19 ч., в т.ч. лекционных – 6 ч., практических – 6 ч., самостоятельная работа – 6 ч., тестирование по модулю – 1 ч

**Лекция (2 ч.) Обеспечение информационной безопасности и безопасности детей в сети Интернет.**

Правовые механизмы по охране и защите детей от информации**.** Структура полномочий надзорных органов.

**Лекция (2 ч.) Защита детей от доступа к негативной информации.**

Обеспечение защиты детей от негативной информации в сети Интернет**.** Виртуальные риски с использованием персональных данных**.** Коммуникационные риски. Риски, связанные с нарушением безопасности**.** Советы родителям: как сделать интернет безопасной территорией для детей.

**Лекция (2 ч.) Всероссийский интернет-урок "Безопасность детей в Интернете": принципы, методы и формы организации.**

Организация режима работы на компьютере. Организация режима доступа к образовательным ресурсам Интернет. Обеспечение информационной безопасности работы в Интернет. Организационно-методические условия обеспечения безопасного ИОП в ОШ Основные организационные и организационно-технические мероприятия Факультативная программа «Медиабезопасность».

**Практическая работа (6 ч.)**

Обучение учащихся правилам безопасной работы в сети: практический инструментарий. Придумать и составить план-график мероприятий и описать часть любого мероприятия в рамках недели: «Безопасный Интернет» в образовательной организации по месту работы слушателя КПК.

**Самостоятельная работа (2 ч.)**

Изучить следующие материалы: Плакаты и инфографика. Методические рекомендации и советы. Нормативные документы. Азбука информационной безопасности. Обеспечение информационной безопасности.

**Самостоятельная работа (2 ч.)**

Изучить видео материалы: Урок безопасного интернета для школьников, Безопасность школьников в сети Интернет.

**Самостоятельная работа (2 ч.)**

Изучить видео материалы: Видео урок для Единого урока безопасности в сети Интернет ЛН Бокова.

5. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ

**5.1. Материально-техническое оснащение курса**

При организации образовательного процесса по программе профессионального обучения в целях реализации компетентностного подхода используются интерактивные технологии, ориентированные на овладение слушателями способов самостоятельной деятельности, личностно-ориентированные технологи, способствующие развитию активности личности обучающегося в учебном процессе.

Слушатели, планирующие обучение с применением дистанционных технологий, должны иметь в своем распоряжении персональный компьютер, доступ в интернет, персональный адрес электронной почты и соответствующие навыки компьютерной грамотности.

Все взаимодействие со слушателями рассылка новостей, информационные материалы, техническая поддержка и пр. осуществляется только по электронной почте.

Одновременно с этим, слушатели получают по электронной почте регистрационный идентификатор логин и пароль доступа к своей персональной странице в системе дистанционного обучения, на которой расположены календарный план обучения, электронные образовательные материалы, методические указания, тестовые контрольные ресурсы и др.

Рекомендуемое программное обеспечение: установленные программы:

* Офисные пакеты: OpenOffice, MS Office или другой
* Минимальные версии веб-браузеров: Coogle Chrome 11, Opera 9.
* AdobeAcrobatReader или аналогичный для просмотра PDF файлов.
* Архиватор 7zip или аналогичные.

5.2. Учебно-методическое и информационное обеспечение курса

5.2.1. Организационно-методическое и информационное обеспечение программы Нормативные документы

1. Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 г. №273-ФЗ (с изменениями и дополнениями)

2. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»

3. Приказ Министерства образования и науки Российской Федерации от 17.12.2010 г. №1897 «Об утверждении федерального государственного образовательного стандарта основного общего образования» (с изменениями и дополнениями)

4. Приказ Министерства образования и науки Российской Федерации от 17.05.2012 г. №413 «Об утверждении федерального государственного образовательного стандарта среднего общего образования» (с изменениями и дополнениями)

5. Приказ Минобрнауки России от 06.10.2009 г. № 373 «Об утверждении и введении в действие федерального государственного образовательного стандарта начального общего образования» (с изменениями и дополнениями)

6. Приказ Министерства труда и социальной защиты Российской Федерации от 18.10.2013 г. №544 н «Об утверждении профессионального стандарта «Педагог» (педагогическая деятельность в сфере дошкольного, начального общего, основного общего, среднего общего образования) (воспитатель, учитель) (с изменениями и дополнениями)

7. Приказ Министерства образования и науки Российской Федерации «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам» от 01.07.2013 г. №499 (ред. от 15 ноября 2013 г.)

8. Концепция информационной безопасности детей, утвержденная распоряжением Правительства Российской Федерации от 02.12.2015 № 2471

5.2.2. Литература

5.2.2.1. Основная литература.

1. Борисов М. А., Романов О. А. Основы организационно-правовой защиты информации. Санкт-Петербург : Ленанд, 2021. 312с.
2. Мельников В. П., Куприянов А. И. Информационная безопасность: учебник. Москва : КноРус, 2021. 272с.
3. Нестеров С. А. Информационная безопасность: учебник и практикум . Санкт-Петербург : Лань, 2021. 324с.
4. Шаньгин В. Ф. Информационная безопасность и защита информации. Москва : ДМК, 2018. 702 c.

5.2.2.2. Дополнительная литература:

1. Баринов В. В. , Баринов И. В. , Пролетарский А. В. , Пылькин А. Н. Компьютерные сети. –М.: ИЦ «Академия» 2018.
2. Гендина Н. И., Косолапова Е. В. Основы информационной культуры школьника : учебно-методический комплекс для учащихся 8-9-х классов общеобразовательных организаций : в 2 ч. Ч. 1. Москва : РШБА, 2020. 272 с.
3. Гендина Н. И., Косолапова Е. В. Основы информационной культуры школьника : учебно-методический комплекс для учащихся 8-9-х классов общеобразовательных организаций : в 2 ч. Ч. 2. Москва : РШБА, 2020. 312 с.
4. Гродзенский Я. С. Информационная безопасность: учебное пособие. Москва : Проспект, 2021. 144с.
5. Ищейнов В. Я. Информационная безопасность и защита информации. теория и практика: учебное пособие. Москва : Директмедиа Паблишинг, 2020. 272с.
6. Партыка Т. Л., Попов И. И. Информационная безопасность: учебное пособие. Москва : Форум, 2018. 88 c.

5.2.2.3. Электронные обучающие материалы

1. Научная электронная библиотека elibrary.ru [Электронный ресурс]/ Основы
2. организационно-правовой защиты информации М.А. Борисов, О.А. Романов: Москва. URSS. [сайт] URL: https://elibrary.ru/item.asp?id=19846872 (дата обращения: 10.04.22)

5.2.2.4. Интернет-ресурсы

1. Безопасный Интернет для детей: законодательство, советы, международный Опыт [Электронный ресурс] : [сайт] URL: www.i-deti.org (дата обращения: 01.04.22)

2. Дети РоссииОнлайн. Сделаем интернет безопаснее вместе [Электронный ресурс] / Сайт проектов Фонда Развития Интернет. - Электрон. текстовые дан. [сайт] URL: http://detionline.com/ (дата обращения: 01.04.22г.).

3. Информационная безопасность образовательного учреждения [Электронный ресурс]: Vladimir:Портал профессиональных сетевых сообществ. [сайт] URL: http://wiki.vladimir.i- edu.ru/ (дата обращения: 01.04.2022 г.).

4. О персональных данных [Электронный ресурс] : федеральный закон от 27.07.2006 г. № 152-ФЗ (ред. от 27.07.2006 г.) // КонсультантПлюс. Москва, 1992. [сайт] URL: http://www.consultant.ru/ (дата обращения: 01.04.2022 г.).

6. ФОРМЫ АТТЕСТАЦИИ

**Промежуточная аттестация**

Промежуточная аттестация проводится по итогам каждого учебного модуля программы в соответствии с учебным планом и календарным учебным графиком образовательной программы. Формы промежуточной аттестации –тестирование.

**Итоговая аттестация**

Итоговая аттестация позволяет выявлять уровень теоретической и практической подготовки слушателей в соответствии с требованиями программы. Итоговая аттестация проводится в форме тестирования.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И ИНЫЕ КОМПОНЕНТЫ

|  |  |  |
| --- | --- | --- |
| **Вид работы** | **Тема работы** | **Ожидаемые результаты, демонстрируемые слушателем при выполнении данного вида работы** |
| Тестирование по модулю 1 | Информационная безопасность в ОО исторические предпосылки, основные понятия и определения | Тестовые задания включают в себя 15 вопросов. Каждый вопрос содержит несколько вариантов ответов, из которых верным(ми) являются от одного до четырех. Время выполнения задания: 30 минут.**Критерии оценивания:**Максимальный балл по тестированию составляет 15. На каждый вопрос засчитывается поодному баллу при условии выбора всех верных вариантов ответа |
| Тестирование по модулю 2 | Информационная безопасность компьютеров, локальной сети, сервисов и информационных систем. | Тестовые задания включают в себя 15 вопросов. Каждый вопрос содержит несколько вариантов ответов, из которых верным(ми) являются от одного до четырех. Время выполнения задания: 30 минут.**Критерии оценивания:**Максимальный балл по тестированию составляет 15. На каждый вопрос засчитывается по одному баллу при условии выбора всех верных вариантов ответа |
| Тестирование по модулю 3 | Организационные меры по защите информации: создание нормативных документов и регламентов | Тестовые задания включают в себя 15 вопросов. Каждый вопрос содержит несколько вариантов ответов, из которых верным(ми) являются от одного до четырех. Время выполнения задания: 30 минут.**Критерии оценивания:**Максимальный балл по тестированию составляет 15. На каждый вопрос засчитывается по одному баллу при условии выбора всех верных вариантов ответа |
| Тестирование по модулю 4 | Обучение учащихся правилам безопасной работы в сети: практический инструментарий. | Тестовые задания включают в себя 15 вопросов. Каждый вопрос содержит несколько вариантов ответов, из которых верным(ми) являются от одного до четырех. Время выполнения задания: 30 минут.**Критерии оценивания:** Максимальный балл по тестированию составляет 15. На каждый вопрос засчитывается по одному баллу при условии выбора всех верных вариантов ответа |
| Итоговое тестирование |  | Тестовые задания включают в себя 20 вопросов. Каждый вопрос содержит несколько вариантов ответов, из которых верным(ми) являются от одного до четырех. Время выполнения задания: 60 минут.**Критерии оценивания:** Максимальный балл по тестированию составляет 20. На каждый вопрос засчитывается по одному баллу при условии выбора всех верных вариантов ответа |