МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КУРСКОЙ ОБЛАСТИ

ОБЛАСТНОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

«КУРСКИЙ ТЕХНИКУМ СВЯЗИ»

|  |  |
| --- | --- |
|  | УТВЕРЖДАЮ  Директора ОБПОУ «КТС»  \_\_\_\_\_\_\_\_\_\_\_\_ А.А. Грунева  *(подпись)*  « \_\_\_\_\_ » \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_\_г. |

**Дополнительная общеразвивающая программа**

**для обучения детей и взрослых**

**Информационная безопасность**

Курск, 2023

|  |  |
| --- | --- |
| РАССМОТРЕНО  на заседании методической комиссии  Протокол №  От « » 2023 г.  Председатель методической комиссии  \_\_\_\_\_\_\_\_\_\_ Кудюров Е.М. |  |

Разработана в соответствии с:

* Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации».
* Приказ Министерства образования и науки Российской Федерации от 23 августа 2017 г. № 816 «Об утверждении порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ».
* Методические рекомендации по разработке основных профессиональных образовательных программ и дополнительных профессиональных программ с учетом соответствующих профессиональных стандартов, утвержденные Министром образования и науки Российской Федерации Д.Л. Ливановым 22 января 2015 г. № ДЛ-1/05вн.
* Письмо Министерства образования и науки Российской Федерации от 10 апреля 2014 г. № 06-381 «О направлении Методических рекомендаций по использованию дистанционных образовательных технологий при реализации дополнительных профессиональных образовательных программ».
* Профессионального стандарта 06.033 Специалист по защите информации в автоматизированных системах (утвержден приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 525н:).

**Разработчик:** Кудюров Евгений Михайлович – преподаватель дисциплин профессионального цикла ОБПОУ «Курский техникум связи»

1. **Дополнительная общеразвивающая программа для обучения детей и взрослых «Информационная безопасность»** 
   1. **Цели реализации программы**

Дополнительная общеразвивающая программа для обучения детей и взрослых «Информационная безопасность» направлена на получение компетенции, необходимой для выполнения нового вида профессиональной деятельности, приобретение новой квалификации, с учетом спецификации ФГБОУ ДПО «Институт развития профессионального образования» по компетенции «Информационная безопасность».

1. **Требования к результатам обучения. Планируемые результаты обучения**

**2.1. Характеристика нового вида профессиональной деятельности, трудовых функций и (или) уровней квалификации**

|  |  |
| --- | --- |
| **№ п/п** | **Содержание вновь формируемой компетенции** |
| 1 | Осуществлять обработку, хранение и передачу информации ограниченного доступа |

К освоению программы допускаются лица, не имеющие основного общего образования, имеющие или получающие среднее профессиональное и (или) высшее образование. Медицинские ограничения регламентированы Перечнем медицинских противопоказаний Минздрава России.

Рабочие места, которые возможно занять по итогам обучения по программе (трудоустройство на вакансии в организации, самозанятость, работа в качестве индивидуального предпринимателя): младший системный администратор, специалист технической поддержки, инженер вычислительных сетей.

**2.2. Требования к результатам освоения программы**

В результате освоения дополнительной профессиональной программы у слушателя должны быть сформированы компетенции, в соответствии с разделом 2.1. программы.

В результате освоения программы слушатель должен:

***знать:***

* особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных;
* типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации;
* общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой серверной операционной системы информационно-коммуникационной системы.

***уметь:***

– применять программные и программно-аппаратные средства для защиты информации;

– проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации.

Трудоемкость обучения: 36 академических часов.

Форма обучения: очная или очная с применением дистанционных образовательных технологий.

* 1. **Учебный план**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№** | **Наименование модулей** | **Всего, ак.час.** | **В том числе** | | | **Форма контроля** |
| **лекции** | **практ. занятия** | **промеж. и итог.контроль** |
| ***1*** | ***2*** | ***3*** | ***4*** | ***5*** | ***6*** | ***7*** |
| 1 | Модуль 1. Теоретические основы информационной безопасности | 16 | 7 | 8 | 1 | Зачет |
| 2 | Модуль 2. Методология защиты информации | 19 | 8 | 10 | 1 | Зачет |
| 3 | Итоговая аттестация | 1 |  |  | 1 | зачет |
|  | **ИТОГО:** | **36** | **17** | **20** | **1** |  |

**2.2. Рабочий тематический план**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Наименование модулей, разделов и тем** | **Содержание учебного материала, лабораторные и практические работы** | | | **Объем часов** |
| **1** | **2** | | | **3** |
| **Модуль 1.** | **Теоретические основы информационной безопасности** | | | **16** |
| **Тема 1.1.**  **Основные**  **понятия и задачи**  **информационной**  **безопасности** | **Содержание учебного материала** | | | **5** |
| Понятие информации и информационной безопасности. | | | 1 |
| Информация, сообщения, информационные процессы как объекты информационной безопасности. | | | 1 |
| Обзор защищаемых объектов и систем.  Понятие «угроза информации». Понятие «риска информационной безопасности». | | | 1 |
| **Практическое занятие** | | | **2** |
|  | | Оценка риска от неинформированности в области информационной безопасности | 2 |
| **Тема 1.2.**  **Основы защиты**  **информации** | **Содержание учебного материала** | | | **6** |
| Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации. | | | 1 |
| Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.  Цели и задачи защиты информации. Основные понятия в области защиты информации. | | | 1 |
| **Практическое занятие** | | | **4** |
| 2. | Определение объектов защиты на типовом объекте информатизации. | | 2 |
| 3. | Классификация защищаемой информации по видам тайны и степеням конфиденциальности. | | 2 |
| **Тема 1.3.**  **Угрозы безопасности**  **защищаемой**  **информации.** | **Содержание учебного материала** | | | **4** |
| Понятие угрозы безопасности информации | | | 1 |
| Системная классификация угроз безопасности информации. | | | 1 |
| **Практическое занятие** | | | **2** |
| 4. | Определение угроз объекта информатизации и их классификация | | 2 |
| **Промежуточная аттестация: Зачет** | | | | **1** |
| **Модуль 2** | **Методология защиты информации** | | | **19** |
| **Тема 2.1. Методологические**  **подходы к защите**  **информации** | **Содержание учебного материала** | | | **5** |
| Анализ существующих методик определения требований к защите информации. | | | 1 |
| Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.  Виды мер и основные принципы защиты информации. | | | 2 |
| **Практическое занятие** | | | **2** |
| 5. | | Оценка факторов, влияющих на требуемый уровень защиты информации. | 2 |
| **Тема 2.2. Нормативно-**  **правовое регулирование**  **защиты информации** | **Содержание учебного материала** | | | **8** |
| Организационная структура системы защиты информации  Законодательные акты в области защиты информации. | | | 2 |
| Российские и международные стандарты, определяющие требования к защите информации.  Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации | | | 2 |
| **Практическое занятие** | | | **4** |
| 6. | | Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности | 2 |
| 7. | | Анализ стандартов в области защиты информации | 2 |
| **Тема 2.3.**  **Защита**  **информации в**  **автоматизированных**  **(информационных)**  **системах** | **Содержание учебного материала** | | | **5** |
| Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах. | | | 1 |
| **Практическое занятие** | | | **4** |
| 8. | | Выбор мер защиты информации для автоматизированного рабочего места | 2 |
| 9. | | Разработка организационно-распорядительной защиты информации | 2 |
| **Промежуточная аттестация: зачет** | | | | **1** |
| **Итоговая аттестация: зачет** | | | | **1** |
| **Всего:** | | | | **36** |

**3.4. Календарный учебный график (порядок модулей)**

**4 недели**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Наименование модулей** | **Трудоемкость, час.:** | **Учебные дни, недели (месяцы)** | | | | | | | | | | | | | |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** |
| Модуль 1. Теоретические основы информационной безопасности | **16** | 10 | 6 |  |  |  |  |  |  |  |  |  |  |  |  |
| Модуль 2. Методология защиты информации | **19** |  | 4 | 10 | 5 |  |  |  |  |  |  |  |  |  |  |
| Итоговая аттестация | **1** |  |  |  | 1 |  |  |  |  |  |  |  |  |  |  |

1. **Организационно-педагогические условия реализации программы**
   1. **Материально-технические условия реализации программы**

Материально-техническое оснащение рабочего места преподавателя программы:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Вид занятий | Наименование  помещения | Наименование оборудования | Количество | Технические характеристики, другие комментарии (при необходимости) |
| *1* | *2* | *3* | *4* | *5* |
| Лекции | Аудитория | Компьютер, мультимедийный проектор, экран, доска | 1 |  |
| Лабораторные и практические занятия, тестирование. | Компьютерный класс | Компьютер, Сервер | По количеству учащихся |  |

Материально-техническое оснащение рабочего места слушателя программы:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Вид занятий | Наименование  помещения | Наименование оборудования | Количество | Технические характеристики, другие комментарии (при необходимости) |
| *1* | *2* | *3* | *4* | *5* |
| Лекции | Аудитория | Стол учебный, стул. | По количеству учащихся |  |
| Лабораторные и практические занятия, тестирование, демонстрационный экзамен | Компьютерный класс | Компьютер, Сервер | По количеству учащихся |  |

* 1. **Учебно-методическое обеспечение программы**
* техническое описание компетенции;
* печатные раздаточные материалы для слушателей;
* учебные пособия, изданных по отдельным разделам программы;
* профильная литература;
* отраслевые и другие нормативные документы;
* электронные ресурсы и т.д.

**Основная литература**

1. Кабанов А. С., Лось А. Б., Сорокин А. В. Основы информационной безопасности, 2021. — 240 c. — ISBN 978-5-4468-9732-2.

**Интернет-ресурсы**

1. CNews: издание о высоких технологиях [Электронный ресурс]. – Режим доступа: http://www.cnews.ru.
2. Intelligententerprise [Электронный ресурс]. – Режим доступа: http://www.iemag.ru.
3. Электронно-библиотечные системы (ЭБС):
4. Лань [Электронный ресурс] – Доступ к данным: открытый. – Режим доступа: http://e.lanbook.com/
5. Университетская библиотека онлайн [Электронный ресурс] – Доступ к данным: открытый. — Режим доступа: http://www.biblioclub.ru/
6. ibooks.ru [Электронный ресурс] – Доступ к данным: открытый. – Режим доступа: http://ibooks.ru/
7. Сетевая академия Cisco [Электронный ресурс]. – Peжим доступа: http://netacad.com.
   1. **Кадровые условия реализации программы**

Количество педагогических работников (физических лиц), привлеченных для реализации программы \_\_\_чел. Из них:

*Ведущий преподаватель программы принимает участие в реализации всех тем и занятий программы.*

**4. Контроль и оценка результатов освоения**

|  |  |
| --- | --- |
| **Результаты обучения**  **(освоенные умения, усвоенные знания)** | **Формы и методы контроля и оценки результатов обучения** |
| В результате освоения дисциплины обучающийся должен **уметь:** |  |
| * применять программные и программно-аппаратные средства для защиты информации; | Выполнение ПЗ 1-9 |
| * проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации. | Выполнение ПЗ 1-9 |
| В результате освоения дисциплины обучающийся должен **знать:** |  |
| * особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; | Модуль 1-2 |
| * типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; | Модуль 1-2 |
| * общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой серверной операционной системы информационно-коммуникационной системы. | Модуль 1-2 |

Оценочные материалы для итоговой аттестации

Вопрос 1:

Кто является основным ответственным за определение уровня классификации информации?

а) Руководитель среднего звена

б) Высшее руководство

в) Владелец

г) Пользователь

Вопрос 2:

Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

а) Сотрудники

б) Хакеры

в) Атакующие

г) Контрагенты (лица, работающие по договору)

Вопрос 3:

Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования

б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

в) Улучшить контроль за безопасностью этой информации

г) Снизить уровень классификации этой информации

Вопрос 4:

Что самое главное должно продумать руководство при классификации данных?

а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

б) Необходимый уровень доступности, целостности и конфиденциальности

в) Оценить уровень риска и отменить контрмеры

г) Управление доступом, которое должно защищать данные

Вопрос 5:

Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

а) Владельцы данных

б) Пользователи

в) Администраторы

г) Руководство

Вопрос 6:

Что такое процедура?

а) Правила использования программного и аппаратного обеспечения в компании

б) Пошаговая инструкция по выполнению задачи

в) Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

г) Обязательные действия

Вопрос 7:

Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

а) Поддержка высшего руководства

б) Эффективные защитные меры и методы их внедрения

в) Актуальные и адекватные политики и процедуры безопасности

г) Проведение тренингов по безопасности для всех сотрудников

Вопрос 8:

Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

а) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски

б) Когда риски не могут быть приняты во внимание по политическим соображениям

в) Когда необходимые защитные меры слишком сложны

г) Когда стоимость контрмер превышает ценность актива и потенциальные потери

Вопрос 9:

Что такое политики безопасности?

а) Пошаговые инструкции по выполнению задач безопасности

б) Общие руководящие требования по достижению определенного уровня безопасности

в) Широкие, высокоуровневые заявления руководства

г) Детализированные документы по обработке инцидентов безопасности

Вопрос 10:

Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

а) Анализ рисков

б) Анализ затрат / выгоды

в) Результаты ALE

г) Выявление уязвимостей и угроз, являющихся причиной риска

Вопрос 11:

Что лучше всего описывает цель расчета ALE?

а) Количественно оценить уровень безопасности среды

б) Оценить возможные потери для каждой контрмеры

в) Количественно оценить затраты / выгоды

г) Оценить потенциальные потери от угрозы в год

Вопрос 12:

Тактическое планирование – это:

а) Среднесрочное планирование

б) Долгосрочное планирование

в) Ежедневное планирование

г) Планирование на 6 месяцев

Вопрос 13. Основными характеристиками защищаемой информации являются:

a) конфиденциальность, целостность и статичность;

b) конфиденциальность, целостность и доступность;

c) аутентификация, целостность и доступность;

d)аутентификация, статичность и время создания;

Вопрос 14. Известность содержания информации только имеющим соответствующие полномочия субъектам – это:

a) Целостность;

b) Статичность;

c) Конфиденциальность;

d) Аутентификация;

Вопрос 15. Неизменность информации в условиях её случайного и (или) преднамеренного искажения и разрушения – это:

a) Целостность;

b) Конфиденциальность;

c) Доступность;

d) Идентификация;

Вопрос 16. Возможность получения информации или информационной услуги за приемлемое время – это:

a) конфиденциальность;

b) целостность;

c) доступность;

d) статичность;

Вопрос 17. Потенциально возможное событие, действие, процесс или явление, которое может привести к изменению функционирования компьютерной системы:

a) уязвимость;

b) атака;

c) угроза;

d) нет верного ответа;

Вопрос 18. Возможность возникновения на каком-либо этапе жизненного цикла компьютерной системы такого её состояния, при котором создаются условия для реализации угроз безопасности информации - это:

a) атака;

b) угроза;

c) уязвимость;

d) статичность;

Вопрос 19. Действия, предпринимаемые злоумышленником, которые заключаются в поиске и использовании уязвимостей информации – это:

a) статичность;

b) атака;

c) угроза;

d) изъян;

Вопрос 20. Классификацию угроз ИБ можно выполнить по нескольким критериям:

a) по аспекту информационной безопасности;

b) по компонентам информационной системы;

c) по способу осуществления;

d) все ответы верны;

9. Конфиденциальная информация может быть разделена на:

a) предметную и служебную;

b) служебную и закрытую;

c) предметную и открытую;

d) открытую и закрытую;

Вопрос 21. Целостность информации может быть разделена на:

a) статическую и динамическую;

b) статическую и служебную;

c) служебную и динамическую;

d) все верно;

Вопрос 22. Примером нарушения статической целостности не является:

a) ввод неверных данных;

b) несанкционированное изменение данных;

c) изменение программного модуля вирусом;

d) внесение дополнительных пакетов в сетевой трафик;

Вопрос 23. Примером нарушения динамической целостности не является:

a) нарушение атомарности транзакций;

b) внесение дополнительных пакетов в сетевой трафик;

c) несанкционированное изменение данных;

d) дублирование данных;

Вопрос 24. Угроза отказа служб может быть разбита на следующие типы:

a) отказ пользователей;

b) внутренний отказ информационной системы;

c) отказ поддерживающей инфраструктуры;

d) все ответы верны;

Вопрос 25. Что не относится к внутреннему отказу ИС:

a) ошибки при переконфигурировании системы;

b) отказы программного и аппаратного обеспечения;

c) разрушение данных;

d) нарушение работы систем связи;

**Практическое задание:** Разработать концепцию информационной безопасности компании, содержащую следующие основные пункты (приведен примерный план, в который в случае необходимости могут быть внесены изменения):

1. Общие положения

1.1. Назначение Концепции по обеспечению информационной безопасности.

1.2. Цели системы информационной безопасности

1.3. Задачи системы информационной безопасности.

2. Проблемная ситуация в сфере информационной безопасности

2.1. Объекты информационной безопасности.

2.2. Определение вероятного нарушителя.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационной безопасности Предприятия.

2.5 Классификации угроз.

2.6 Основные непреднамеренные искусственные угрозы.

2.7 Основные преднамеренные искусственные угрозы.