НПОУ «ЯКУТСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

УТВЕРЖДЕНО
педагогическим советом
(протокол № 03-23 от «29» марта 2023)
Председатель педагогического совета
Директор _____Л.Н. Цой

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА

(Повышение квалификации)

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ НАЧИНАЮЩИХ»

Объем курса – 72 часа

СОГЛАСОВАНО
на заседании методического совета
НПОУ «ЯКИТ»
(протокол № 03-23 от «22» марта 2023)
Председатель _____ С.И. Томская

Якутск, 2023

СОДЕРЖАНИЕ

1. ОБЛАСТЬ ПРИМЕНЕНИЯ ПРОГРАММЫ

Программа «Основы информационной безопасности для начинающих» относится к программам повышения квалификации.

Курс повышения квалификации в области информационной безопасности разработан с учётом требований Федерального закона от 28 декабря 2010 г. № 390-ФЗ «О безопасности», Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Основой для разработки программы являются Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», а также документы ФСТЭК России, регламентирующие вопросы обеспечения безопасности персональных данных: «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», «Методический документ. Методика оценки угроз безопасности информации» от 05.02.2021 г. и «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные приказом ФСТЭК России от 18 февраля 2013 № 21.

Цель курса

Формирование знаний и навыков, необходимых для организации и обеспечения безопасности персональных данных, обрабатываемых в информационных системах государственных, муниципальных органов, органов местного самоуправления и организаций различных форм собственности, физических лиц, организующих и (или) осуществляющих обработку персональных данных.

Целевая аудитория:

– физические лица, организующие и (или) осуществляющие обработку персональных данных;

– руководители и сотрудники организаций различных форм собственности, организующие обработку персональных данных.

Требования к слушателям:

– знать основы информационных технологий;

– иметь навыки работы на персональном компьютере в ОС семейства MS Windows;

– иметь навыки работы в пакете MS Office 2010 или выше.

После успешного освоения курса слушатель будет:

ЗНАТЬ:

– основные положения нормативных правовых актов, регламентирующих вопросы обеспечения безопасности персональных данных;

– основные виды угроз безопасности персональных данных в информационных системах персональных данных;

– содержание и порядок организации работ по определению и оценке угроз безопасности персональных данных;

– процедуры задания и реализации требований по защите информации в информационных системах персональных данных;

– меры обеспечения безопасности персональных данных;

– требования по обеспечению безопасности персональных данных;

– порядок применения организационных мер и технических средств обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.

УМЕТЬ:

– создавать организационно-распорядительные документы в интересах организации работ по обеспечению безопасности персональных данных;

– планировать мероприятия по обеспечению безопасности персональных данных;

– обосновывать и задавать требования по обеспечению безопасности персональных данных в информационных системах персональных данных;

– проводить оценку угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

– определять состав и содержание мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для блокирования угроз безопасности персональных данных.

ВЛАДЕТЬ:

– навыками работы с правовыми базами данных;

– навыками определения уровней защищённости персональных данных;

– навыками определения и оценки угроз безопасности персональных данных в информационных системах персональных данных;

– навыками разработки и реализации организационных мер, обеспечивающих эффективность системы защиты информации;

– навыками разработки модели угроз безопасности персональным данным в организации;

– навыками разработки необходимых документов в интересах организации работ по обеспечению безопасности персональных данных;

– навыками применения сертифицированных средств защиты информации.

Успешное окончание курса по программе курса позволит специалистам:

– эффективно организовывать процесс обработки персональных данных в организации (компании);

– проводить обследование (принимать участие в обследовании) информационных систем организации с целью определения сведений, необходимых для построения системы защиты персональных данных;

– определять и оценивать угрозы безопасности персональных данных в информационных системах персональных данных и оценивать степень их опасности;

– самостоятельно определять требуемые уровни защищённости персональных данных, обрабатываемых в информационных системах персональных данных;

– определять и обосновывать необходимость применения средств защиты информации;

– аргументированно выбирать средства защиты информации, удовлетворяющие потребностям организации – обладателя информации;

– правильно организовать эксплуатацию средств защиты информации;

– самостоятельно разрабатывать требуемую организационно-распорядительную документацию.

Программа курса включает как лекционные занятия (предусмотрен дистанционный формат), так и значительный объем практических занятий (только очно).

К прохождению курса допускаются лица имеющие среднее профессиональное образование или высшее образование.

Программа рассчитана на 72 часа и включает в себя:

1. Методологические основы информационной безопасности *Организационно-правовое обеспечение ИБ:*

– теория информационной безопасности и методология защиты информации;

– правовое, нормативное и методическое регулирование деятельности в области защиты информации;

– правовые основы организации защиты государственной тайны, задачи органов защиты государственной тайны;

2. Основные направления безопасности инфраструктуры. Комплексный подход к защите организации;

3. Аспекты безопасности локальной сети и беспроводных систем;

4. Сетевые экраны. Сетевые атаки и анализ трафика;

5. Системы отчетности. Средства обнаружения и утечек данных;

6. Аспекты безопасности веб-приложений;

7. Криптографическая защита информации:

– криптографические методы защиты информации;

– обеспечение применения электронной подписи и инфраструктуры открытого ключа с использованием сертифицированных средств;

8. Организация обработки персональных данных (далее ПДн):

– нормативное правовое регулирование организации обработки и обеспечения безопасности персональных данных в российской федерации;

– основные положения ФЗ-152 «О персональных данных»;

– меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

– организация работ и назначение ответственных лиц;

– прием и обработка обращений и запросов субъектов персональных данных или их представителей;

– обследование информационных систем организации и описание процессов обработки персональных данных;

– определение перечня, категории и объёма обрабатываемых персональных данных, категории субъектов, ПДн которых обрабатываются, способов обработки персональных данных;

– проблемные вопросы отнесения фото- и видео- изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки;

– определение правового основания обработки персональных данных и прочих сведений, необходимых для регистрации организации в реестре Роскомнадзора;

– определение перечня информационных систем персональных данных;

– определение перечня должностей сотрудников, допущенных к обработке персональных данных в организации;

– политика в отношении обработки персональных данных в организации;

– ознакомление работников с порядком обработки и обеспечения безопасности персональных данных;

– согласие на обработку персональных данных;

– разработка типового согласия на обработку персональных данных сотрудников организации и иных субъектов персональных данных;

– разъяснение субъекту ПДн юридических последствий отказа предоставить свои ПДн;

– порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных;

– организация обработки персональных данных, осуществляемой без использования средств автоматизации;

– требования и методы по обезличиванию персональных данных;

– требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных;

– уведомление уполномоченного органа по защите прав субъектов персональных данных об обработке (намерении осуществлять обработку) персональных данных;

– осуществление внутреннего контроля соответствия обработки персональных данных установленным требованиям.

2. УЧЕБНЫЙ ПЛАН ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

№ п\п	Дисциплина/вид занятия	Количество часов		Форма контроля
		Лекции	Практические	
1	Методологические основы информационной безопасности. Организационно-правовое обеспечение ИБ.	2	-	Зачет
2	Основные направления безопасности инфраструктуры. Комплексный подход к защите организации.	2	-	Зачет
3	Аспекты безопасности локальной сети и беспроводных систем	2	14	Зачет
4	Сетевые экраны. Сетевые атаки и анализ трафика	2	10	Зачет
5	Системы отчетности. Средства обнаружения и утечек данных	2	10	Зачет
6	Аспекты безопасности веб-приложений	2	-	Зачет
7	Криптографическая защита информации	2	12	Зачет
8	Организация обработки персональных данных	2	-	Зачет
9	Самостоятельная работа	-	8	-
10	Итоговый контроль		2	Защита проекта
11	ЧАСОВ:	16	46	-
12	ИТОГО ЧАСОВ:	72		-

Форма итогового контроля

Для успешного завершения курсов повышения квалификации слушателю необходимо подготовить и презентовать проект по разработке системы информационной безопасности организации.

После успешного завершения курсов слушатель получает Удостоверение установленного образца.

Список рекомендуемых источников:

1 Сети и телекоммуникации : учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.] ; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2023. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/517817 (дата обращения: 03.04.2023).

2 Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 1 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2023. — 333 с. — (Профессиональное образование). — ISBN 978-5-534-04638-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/513518 (дата обращения: 03.04.2023).

3 Дибров, М. В. Компьютерные сети и телекоммуникации. Маршрутизация в IP-сетях в 2 ч. Часть 2 : учебник и практикум для среднего профессионального образования / М. В. Дибров. — Москва : Издательство Юрайт, 2023. — 351 с. — (Профессиональное образование). — ISBN 978-5-534-04635-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/514019 (дата обращения: 03.04.2023).

4 Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519364 (дата обращения: 03.04.2023).

5 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,

2023. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/518006 (дата обращения: 03.04.2023).

6 Гафарова, Е.А. Организационно-правовое обеспечение информационной безопасности : учебное пособие / Е.А. Гафарова. - Челябинск : Издательство, 2019 ЗАО «Библиотека А. Миллера». - 153 с.

7 Новиков, В. К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации) : учебное пособие / В. К. Новиков. — Москва : Горячая линия-Телеком, 2017. — 176 с. — ISBN 978-5-9912-0525-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/111084 (дата обращения: 03.04.2023).

8 Информационная безопасность и защита информации: Учебное пособие/Баранова Е. К., Бабаш А. В., 3-е изд.- М.: ИЦ РИОР, НИЦ ИНФРА-М, 2018. - 322 с.

9 Хорев П. Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - М.: Форум, 2020. -352 с.

10 Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2023. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512861 (дата обращения: 03.04.2023).

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО ОБУЧЕНИЯ

Требования к материально-техническому оснащению программы

Помещения должны представлять собой учебные аудитории для проведения занятий всех видов, предусмотренных программой профессионального обучения, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы, мастерские и лаборатории, оснащенные оборудованием, техническими средствами обучения.

Материально - техническое оснащение лабораторий, мастерских и баз практики по профессии.

Реализация программы профессионального обучения предполагает наличие оснащенного кабинета, который включает в себя:

- мультимедийный проектор;
- проекционный экран;
- принтер лазерный;
- компьютерная техника;
- столы, стулья;
- компьютеры на рабочем месте учащихся с наличием лицензионного обеспечения.