Частное образовательное учреждение дополнительного профессионального образования «Саранский Дом науки и техники Российского Союза научных и инженерных общественных объединений»

Утверждаю
Директор
ЧОУ ДПО «Саранский Дом
науки и техники РСНИИОО»

_____А.М. Зюзин

«12» февраля 2018 г.

УЧЕБНАЯ ПРОГРАММА
ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА ПОВЫШЕНИЯ КВАЛИФИКАЦИИ
«Система информационной безопасности в организации»
(36 акад. часов)

Цель: овладение теоретическими и практическими знаниями в области информационной безопасности.

Вид деятельности: современные информационные технологии для использования в сфере защиты информации.

Категория слушателей: специалисты по защите информации организаций и учреждений, осуществляющие разработку и эксплуатацию автоматизированных информационных систем, обеспечивающих обработку, хранение и передачу персональных данных.

Продолжительность обучения: 36 часов.

Форма обучения: очная.

Режим занятий: 7-8 часов в день.

Выдаваемый документ: удостоверение о повышении квалификации.

Разработчик программы: зав.учебной частью Зюзина М.В., преподаватель Циликов Н.С.

Саранск 2018

Пояснительная записка.

Дополнительная профессиональная программа повышения квалификации **«Система информационной безопасности в организации»** предназначена для обучения специалистов, отвечающих за эксплуатацию автоматизированных информационных систем, обеспечивающих обработку, хранение и защиту информации.

Цель: изучение государственной системы защиты информации, ее задачи, структуру и перспективы развития; определение способов и средств реализации угроз безопасности информации и их источниках, а также способов и средств технической защиты конфиденциальной информации.

В программе отражены требования нормативных правовых актов и методических документов Федеральной службы по техническому и экспортному контролю (ФСТЭК России) и учтено содержание работ по обеспечению технической защиты информации, проводимых управлениями ФСТЭК России по федеральным округам.

Учебная программа направлена на обеспечение слушателей теоретическими и практическими знаниями по организации и проведению работ по технической защите информации на объектах информатизации в органах государственной власти субъектов РФ, органах местного самоуправления, организациях и учреждениях. Программа направлена на изучение:

организационно-правовых основ технической защиты конфиденциальной информации;

методов и процедур выявления угроз безопасности информации на объектах защиты;

методов оценки состояния технической защиты конфиденциальной информации;

методов и порядка осуществления работ по технической защите конфиденциальной информации.

Основой подготовки специалистов, является изучение основных положений «Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К)», введенных в действие приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

При подготовке специалистов большое внимание придается четкому уяснению их полномочий и практических действий в вопросах технической защиты конфиденциальной информации, их строгому сопоставлению с политикой, проводимой государством в области технической защиты информации.

Планируемые результаты обучения

Слушатели должны знать :

-содержание нормативных правовых актов в области технической защиты конфиденциальной информации;

-методы и процедуры выявления угроз безопасности информации на объектах информатизации;

-порядок организации работ по технической защите конфиденциальной информации на объектах информатизации;

-требования и рекомендации по защите речевой конфиденциальной информации;

-требования и рекомендации по защите конфиденциальной информации, обрабатываемой в автоматизированных системах;

-методы контроля и оценки состояния технической защиты конфиденциальной информации;

Слушатели должны уметь:

-организовывать работы по выявлению угроз безопасности информации на объектах информатизации;

-планировать, организовывать и контролировать выполнение мероприятий по технической защите конфиденциальной информации;

-разрабатывать необходимые документы по организации технической защиты конфиденциальной информации;

-оценивать эффективность защиты конфиденциальной информации;

Слушатели должны владеть:

- навыками работы с нормативными правовыми актами в области обеспечения информационной безопасности;
- методами и средствами выявления угроз личности и информации;
- навыками защиты прав на интеллектуальную собственность;
- навыками организации и обеспечения режима защиты персональных данных;
- навыками выявления и уничтожения компьютерных вирусов;
- навыками безопасного использования технических и программных средств защиты информации в профессиональной деятельности;

-навыками работы с техническими и программными средствами выявления угроз безопасности информации и средствами защиты от этих угроз;

-навыками разработки необходимых документов в интересах организации работ по технической защите конфиденциальной информации.

При разработке программы выполнены требования к содержанию дополнительных профессиональных образовательных программ, утверждённые приказом Министерства образования и науки РФ от 1 июля 2013 г. N 499 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам».

***Категория слушателей*:** руководители органов государственной власти субъектов РФ и органов местного самоуправления субъектов РФ, руководители и специалисты подразделений по защите информации организаций и учреждений.

Требования к слушателям

К освоению программы повышения квалификации допускаются: 1) лица, имеющие среднее профессиональное и (или) высшее образование; 2) лица, получающие среднее профессиональное и (или) высшее образование.

Форма обучения

Форма обучения: очная.

Обучение специалистов проводится в учебных классах, оснащенных компьютерами и мультимедийным оборудованием, что позволяет создавать оптимальные условия для восприятия слушателями учебного материала путем работы с презентационными материалами и нормативными правовыми документами непосредственно за рабочим местом слушателя. Кроме того, методические материалы представлены раздаточными материалами, выдаваемыми каждому слушателю. Каждое рабочее место слушателя снабжено выходом в сеть «Интернет», что позволяет в любой момент времени в соответствии с учебной программой посещать официальные сайты.

По окончании обучения проводится итоговый контроль знаний слушателей в форме тестирования.

Утверждаю
Директор
ЧОУ ДПО «Саранский Дом
науки и техники РСНИИОО»

_____А.М. Зюзин

«12» февраля 2018г.

УЧЕБНЫЙ ПЛАН

обучение по дополнительной профессиональной программе повышения квалификации «Система информационной безопасности в организации»

Рекомендуемый уровень начальной подготовки: высшее образование и среднее профессиональное
Срок обучения: 36 час.
Форма обучения: очная
Выдаваемый документ: удостоверение о повышении квалификации
Режим занятий : 8 час. в день

№ п/п	Наименование разделов, дисциплин и тем	Всего часов	В том числе		
			Лекции	Практические занятия	Формы контроля
1	2	3	4	5	7
1	Нормативно-правовые основы обеспечения информационной безопасности в РФ	**4**	**4**		
2	Комплексная система обеспечения информационной безопасности в организации.	**4**	**4**		текущий
3	Современные угрозы информационной безопасности автоматизированных систем	**6**	**4**	**2**	текущий
4	Техническая защита конфиденциальной информации от ее утечки по техническим каналам	**10**	**6**	**4**	текущий
5	Криптографическая защита конфиденциальной информации. Криптографические системы.	**10**	**6**	**4**	текущий
6.	**Итоговое тестирование**	**2**		**2**	
	ИТОГО	**36**	**24**	**12**	

Форма обучения: Очная
Методика обучения: Лекционные занятия – 24 часов
Практические занятия – 12 часов
Общий объем занятий: **36 час.**

Утверждаю
Директор
ЧОУ ДПО «Саранский Дом науки и техники РСНИИОО»

_____А.М. Зюзин

«12» февраля 2018г.

УЧЕБНО-ТЕМАТИЧЕСКИЙ ПЛАН
обучение по дополнительной профессиональной программе повышения квалификации «Система информационной безопасности в организации»

Рекомендуемый уровень начальной подготовки: высшее образование и среднее профессиональное
Срок обучения: 36 час.
Форма обучения: очная
Выдаваемый документ: удостоверение о повышении квалификации
Режим занятий : 8 час. в день

№ п/п	Наименование разделов, дисциплин и тем	Всего часов	В том числе		
			Лекции	Практические занятия	Формы контроля
1	2	3	4	5	7
1.	**Нормативно-правовые основы обеспечения информационной безопасности в РФ**	**4**	**4**		
1.1	Доктрина информационной безопасности Российской Федерации. Система руководящих и специальных нормативных документов Российской Федерации в области защиты информации	2	2		
1.2	Система лицензирования деятельности, сертификации средств защиты и аттестации объектов информатизации по требованиям законодательства Российской Федерации	2	2		
2.	**Комплексная система обеспечения информационной безопасности в организации.**	**4**	**4**		текущий
2.1	Особенности современного предприятия как объекта защиты информации	1	1		
2.2	Сущность и задачи комплексной защиты информации	1	1		
2.3	Основные стратегии комплексной защиты информации	1	1		
2.4	Основные требования к построению комплексной защиты информации	1	1		

3	**Современные угрозы информационной безопасности автоматизированных систем**	**6**	**4**	**2**	текущий
3.1	Анализ современных угроз информационной безопасности автоматизированных систем их факторы, классификация, характеристика способов и средств их реализации	2	2		
3.2	Основные компоненты комплексной системы обеспечения информационной безопасности в организации	1	1		
3.3	Структура и базовый состав организационно-распорядительной документации организации по информационной безопасности	1	1		
3.4	Модель угроз и модель нарушителя информационной безопасности	2		2	
4	**Техническая защита конфиденциальной информации от ее утечки по техническим каналам.**	**10**	**6**	**4**	текущий
4.1	Технические каналы утечки информации и их характеристики. Технические каналы утечки речевой информации. Утечка информации за счет побочных электромагнитных излучений и наводок	2	1	1	
4.2.	Организация работ по обеспечению комплексной защиты сведений, составляющих конфиденциальную информацию	3	1	2	
4.3.	Пассивные и активные методы, используемые при создании систем защиты информации	3	2	1	
4.4.	Защита информации на автоматизированных рабочих местах на базе автономных ПЭВМ. Защита информации в локальных вычислительных сетях.	2	2		
5	**Криптографическая защита конфиденциальной информации. Криптографические системы.**	**10**	**6**	**4**	текущий
5.1	Место и роль средств криптографической защиты в системе защиты информации организации	1	1		
5.2	Типовые требования к применению средств криптографической защиты информации (размещение, установка, контроль доступа, эксплуатация)	2	2		

5.3	Порядок применения средств криптографической защиты (ввод в эксплуатацию, учет и хранение, эксплуатация, вывод из эксплуатации)	2	2		
5.4	Назначение и основные возможности СКЗИ Крипто-Про Структура ПО Крипто-Про	3	1	2	
5.5	Технологии криптографической защиты информации	2		2	
6.	**Итоговое тестирование**	**2**		**2**	
	ИТОГО	**36**	**24**	**12**	

Форма обучения: Очная
Методика обучения: Лекционные занятия – 24 часов
Практические занятия –12 часов

Общий объем занятий: **36 час.**

I. Содержание программы

1. Нормативно-правовые основы обеспечения информационной безопасности в РФ

Информация, информационные отношения, субъекты информационных отношений, их интересы и пути нанесения им ущерба. Конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации.

Федеральные законы Российской Федерации. Постановления правительства Российской Федерации. Указы Президента Российской Федерации. Ответственность за правонарушения в области защиты информации.

Национальные (ГОСТ), международные и отраслевые стандарты в области защиты информации, информационных технологий и непрерывности бизнеса

Система руководящих и специальных нормативных документов Российской Федерации в области защиты информации. Доктрина информационной безопасности Российской Федерации.

Система руководящих и специальных нормативных документов Российской Федерации в области защиты информации. Система лицензирования деятельности, сертификации средств защиты и аттестации объектов информатизации по требованиям законодательства Российской Федерации.

2. Комплексная система обеспечения информационной безопасности в организации

Особенности современного предприятия как объекта защиты информации.

Сущность и задачи комплексной защиты информации.

Основные стратегии комплексной защиты информации .

Основные требования к построению комплексной защиты информации .

3. Современные угрозы информационной безопасности автоматизированных систем

Анализ современных угроз информационной безопасности автоматизированных систем их факторы, классификация, характеристика способов и средств их реализации.

Основные компоненты комплексной системы обеспечения информационной безопасности в организации.

Модель угроз и модель нарушителя информационной безопасности.

Структура и базовый состав организационно-распорядительной документации организации по информационной безопасности.

4. Техническая защита конфиденциальной информации от ее утечки по техническим каналам

Технические каналы утечки информации и их характеристики. Технические каналы утечки речевой информации. Утечка информации за счет побочных электромагнитных излучений и наводок.

Организация работ по обеспечению комплексной защиты сведений, составляющих

конфиденциальную информацию.

Пассивные и активные методы, используемые при создании систем защиты информации.

Защита информации на автоматизированных рабочих местах на базе автономных ПЭВМ.

Защита информации в локальных вычислительных сетях.

5. Криптографическая защита конфиденциальной нформации. Криптографические системы.

Место и роль средств криптографической защиты в системе защиты информации организации.

Типовые требования к применению средств криптографической защиты информации (размещение, установка, контроль доступа, эксплуатация).

Порядок применения средств криптографической защиты (ввод в эксплуатацию, учет и хранение, эксплуатация, вывод из эксплуатации).

Назначение и основные возможности СКЗИ Крипто-Про.

Структура ПО Крипто-Про. Технологии криптографической защиты информации.

МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОСНАЩЕНИЕ

1. Справочная правовая система Консультант Плюс.
2. Компьютерные классы с мультимедийным оборудованием.
3. Презентационные материалы.
4. Раздаточные материалы: «Система информационной безопасности в организации».

Для реализации указанной программы учреждение имеет мобильные и стационарные компьютерные классы с сетью Интернет, оснащенные программным обеспечением, оргтехнику, специальное оборудование для изготовления полиграфической продукции. Учебное здание, в котором расположены учебные классы, принадлежат учреждению на праве оперативного управления. Все материальные ресурсы принадлежат учреждению на праве собственности.

Календарный учебный график по программе повышения квалификации

«Система информационной безопасности в организации»

Образовательный процесс по программе может осуществляться в течение всего учебного года. Занятия проводятся по мере комплектования групп.

Форма обучения / **График обучения**	**Ауд. часов в день**	**Дней в неделю**	**Общая продолжительность программы (дней, недель, месяцев)**
очная	7-8	5	1 неделя

Период обучения

А	ТК	ИА

Условные обозначения:
А- Аудиторные занятия
ТК- Текущий контроль
ИА- Итоговая аттестация