ЧАСТНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ «ЦЕНТР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ»

ЧУ ДПО "ЦИТ БИС"

Подписано цифровой подписью: ЧУ ДПО "ЦИТ БИС"
DN: email=edu@astralnalog.ru, 1.2.643.3.131.1.1=120C303034303237303936363335, 1.2.643.100.3=120B303038393331313531343 2, 1.2.643.100.1=120D313039343030303030313131353 0, street=ул Циолковского 4 212, c=RU, st=40 Калужская область, l=г Калуга, o=ЧУ ДПО "ЦИТ БИС", title=Директор, givenName=Игорь Ильич, sn=Чернин, cn=ЧУ ДПО "ЦИТ БИС"
Дата: 2022.01.20 10:47:36 +03'00'

УТВЕРЖДАЮ

Директор ЧУ ДПО «ЦИТ БИС»

_____ И.И. Чернин
«___»_____2018г

Программа повышения квалификации

«Техническая защита информации. Способы и средства защиты информации от несанкционированного доступа»

Калуга

2018

1.Общие положения

Настоящая программа повышения квалификации «Техническая защита информации. Способы и средства защиты информации от несанкционированного доступа» (далее - программа повышения квалификации) разработана с учетом положений:

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

приказа Минобрнауки России от 5 декабря 2013 г. № 1310 «Об утверждении порядка разработки дополнительных профессиональных программ, содержащих сведения, составляющие государственную тайну, и дополнительных профессиональных программ в области информационной безопасности»;

приказа Минобрнауки России от 1 июля 2013 г. № 499 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

профессионального стандарта«Специалист по технической защите информации», утвержденного приказом Минтруда России от 1 ноября 2016 г. № 599н;

профессионального стандарта «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденного приказом Минтруда России от 3 ноября 2016 г. № 608н;

профессионального стандарта «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Минтруда России от 1 ноября 2016 г. № 598н;

профессионального стандарта«Специалист по защите информации в автоматизированных системах», утвержденного приказом Минтруда России от 15 сентября 2016 г. № 522н; .

федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата), утвержденного приказом Минобрнауки России от 1 декабря 2016 г. № 1515;

федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.04.01 Информационная безопасность (уровень магистратура), утвержденного приказом Минобрнауки России от 1 декабря 2016 г. № 1513;

федерального государственного образовательного стандарта высшего образования по специальности 10.05.01 Компьютерная безопасность (уровень специалитета), утвержденного приказом Минобрнауки России от 1 декабря 2016 г. № 1512;

федерального государственного образовательного стандарта высшего образования по специальности 10.05.02 Информационная безопасность телекоммуникационных систем (уровень специалитета), утвержденного приказом Минобрнауки России от 16 ноября 2016 г. № 1426;

федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 Информационная безопасность

автоматизированных систем (уровень специалитета), утвержденного приказом Минобрнауки России от 1 декабря 2016 г. № 1509;

Методических рекомендаций по разработке программ профессиональной переподготовки и повышения квалификации специалистов, работающих в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры, противодействия иностранным техническим разведкам и технической защиты информации, утвержденных ФСТЭК России 4 апреля 2015 г.;

Методических рекомендаций-разъяснений по разработке дополнительных профессиональных программ на основе профессиональных стандартов (письмо Минобрнауки России от 22 апреля 2015 г. № ВЖ-1032/06);

примерной программы повышения квалификации «Техническая защита информации. Способы и средства защиты информации от несанкционированного доступа», утвержденной ФСТЭК России 30 марта 2016 г.

2. Цель реализации программы повышения квалификации

Целью реализации программы повышения квалификации является совершенствование и (или) получение новых компетенций, необходимых для осуществления профессиональной деятельности, и (или) повышение профессионального уровня в рамках имеющейся квалификации специалистов (включая государственных гражданских служащих), работающих в области технической защиты информации (ТЗИ) (далее - обучающиеся), в части разработки и применения способов и средств защиты информации от несанкционированного доступа (НСД).

3. Требования к квалификации поступающего на обучение

Уровень образования лица, поступающего на обучение, - среднее или высшее образование по специальностям и направлениям подготовки укрупненной группы 10.00.00 «Информационная безопасность» или профессиональная подготовка по направлению ТЗИ, подтвержденные документом об образовании.

4. Планируемые результаты обучения

В результате освоения программы повышения квалификации обучающиеся должны получить знания, умения и навыки, обеспечивающие совершенствование и (или) получение новых компетенций, необходимых им для осуществления своей профессиональной деятельности.

5. Условия реализации программы

Лабораторная база учреждения оснащена современным оборудованием, стендами, приборами, позволяющими изучать и исследовать аппаратуру и процессы в соответствии с реализуемой программой профессиональной переподготовки.

Компьютерные классы оборудованы современной вычислительной техникой для занятий по учебным дисциплинам из расчета одно рабочее место на одного обучающегося при проведении занятий в данных классах.

6. Формы аттестации

Форма итоговой аттестации обучающихся, освоивших программу повышения квалификации, экзамен в форме тестирования.

7. Учебный план программы повышения квалификации

№ п/п	Наименование учебных модулей, тем	Всего учебных часов	Часы занятий с преподавателем	Распределение времени по видам занятий, час					Самостоятельная работа обучающихся	Формы аттестации и контроля знаний
				Лекции	Семинары	Практические занятия	Лабораторные работы	Промежуточная аттестация		
1	2	3	4	5	6	7	8	9	10	И
1.	Базовая часть	100	74	26	24	12	12	-	26	-
1.1.	Учебный модуль № 1. Организация работ по ТЗИ	40	30	10	14	6	-	-	10	Текущий контроль. Тестирование
1.1.1.	Тема № 1. Цели и задачи ТЗИ	6	4	2	2	-	-	-	2	-
1.1.2.	Тема № 2. Защищаемые информация и информационные ресурсы. Объекты защиты	6	4	2	2	-	-	-	2	-
1.1.3.	Тема № 3. Угрозы безопасности информации, связанные с НСД	10	8	2	2	4	-	-	2	-
1.1.4.	Тема № 4. Правовые основы ТЗИ	10	8	2	6	-	-	-	2	-
1.1.5.	Тема № 5. Формирование требований	8	6	2	2	2	-	-	2	-

1	2	3	4	5	6	7	8	9	10	11
1.2.	Учебный модуль № 2. Защита	24	20	4	8	-	8	-	4	Текущий контроль.
1.2.1.	Тема№ 1. Организационно-технические основы выполнения мероприятий по	6	4	2	2	-	-	-	2	-
1.2.2.	Тема № 2. Меры и средства защиты информации от НСД	18	16	2	6	-	8	-	2	-
1.3.	Учебный модуль № 3. Контроль состояния ТЗИ от НСД	36	24	8	6	6	4	-	12	-
1.3.1.	Тема № 1. Основные задачи контроля состояния ТЗИ от НСД	6	4	2	2	-	-	-	2	Текущий контроль. Тестиро-вание
1.3.2.	Тема № 2. Методы и средства контроля защищенности информации от НСД	12	8	2	-	2	4	-	4	-
1.3.3.	Тема № 3. Аттестация объектов информатизации по требованиям безопасности информации	8	6	2	2	2	-	-	2	-
1.3.4.	Тема № 4. Сертификация средств защиты информации от НСД	10	6	2	2	2	-	-	4	-
2.	Итоговая аттестация	8	2	2	-	-	-	-	6	-
2.1.	Итоговое тестирование	6	-	-	-	-	-	-	6	-
Итого:		108	76	24	28	12	12	-	32	-

8. Примерный календарный учебный график

Срок обучения по программе повышения квалификации, месяцы	1		
Срок обучения по программе повышения квалификации, недели	1	2	
Виды занятий, предусмотренные программой повышения квалификации	А	А	И

А - аудиторная и самостоятельная работа; И итоговая аттестация.

9. Рабочая программа учебного курса

9.1. Содержание учебных модулей, тем

Учебный модуль № 1. Организация работ по ТЗИ.

Тема № 1. Цели и задачи ТЗИ.

Основные термины и определения в области ТЗИ. Государственная система ПД ИТР и ТЗИ. Место ТЗИ в системе мероприятий по обеспечению информационной безопасности в Российской Федерации. Цели и задачи ТЗИ.

Тема № 2. Защищаемые информация и информационные ресурсы. Объекты защиты.

Объекты защиты информации. Защищаемые информация и информационные ресурсы. Объекты информатизации, их классификация и характеристика.

Государственные информационные ресурсы, негосударственные информационные ресурсы, находящиеся в ведении органов государственной власти и организаций.

Тема № 3. Угрозы безопасности информации, связанные с НСД.

Понятие и классификация угроз безопасности информации, связанных с НСД. Источники угроз безопасности информации от НСД.

Модели угроз безопасности информации от НСД.

Методы выявления и анализа угроз безопасности информации, уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах.

Банк данных угроз безопасности информации, включающий базу данных уязвимостей программного обеспечения, используемого в автоматизированных (информационных) системах.

Тема № 4. Правовые основы ТЗИ.

Правовые основы защиты информации. Система документов в области ТЗИ. Нормативные правовые акты. Нормативные правовые акты ФСТЭК России. Методические документы. Технические документы (документация). Плановые документы. Информационные документы. Документы в области технического регулирования и стандартизации. Система стандартов в области защиты информации.

Тема № 5. Формирование требований по защите информации и создание системы защиты информации от НСД.

Формирование требований по защите информации от НСД, содержащейся в информационной системе (на объекте информатизации).

Требования по защите информации от НСД.

Учебный модуль № 2. Защита информации от НСД.

Тема№ 1. Организационно-технические основы выполнения мероприятий по ТЗИ от НСД.

Комплекс мероприятий по ТЗИ от НСД.

Особенности защиты информации от НСД при использовании современных информационных технологий (мобильных, беспроводных, грид, суперкомпьютерных, виртуализации, облачных, больших данных и др.).

Обеспечение защиты информации от НСД в ходе эксплуатации аттестованной

Тема № 2. Меры и средства защиты информации от НСД.

Общая характеристика и классификация мер и средств защиты информации от НСД.

Требования к мерам защиты информации от НСД, реализуемым в автоматизированной (информационной) системе. Меры защиты информации от НСД. Особенности создания системы защиты информации от НСД как обеспечивающей подсистемы автоматизированной (информационной) системы. Системные и документальные части системы защиты информации от НСД.

Учебный модуль № 3. Контроль состояния ТЗИ от НСД.

Тема № 1. Основные задачи контроля состояния ТЗИ от НСД.

Классификация видов контроля состояния ТЗИ от НСД.

Система документов по контролю состояния ТЗИ от НСД.

Вопросы, подлежащие проверке при контроле состояния ТЗИ от НСД в организации.

Организационный и технический контроль состояния ТЗИ от НСД.

Тема № 2. Методы и средства контроля защищенности информации от НСД.

Классификация методов контроля защищенности информации от НСД и их

характеристика. Сканеры безопасности и их характеристика. Средства анализа программных кодов и их характеристика. Средства антивирусной защиты и их характеристика.

Тема № 3. Аттестация объектов информатизации по требованиям безопасности информации.

Порядок проведения аттестации объектов информатизации по требованиям безопасности информации. Программы и методики аттестационных испытаний. Заключение по результатам аттестации объекта информатизации. Аттестат соответствия объекта информатизации.

Тема № 4. Сертификация средств защиты информации от НСД.

Порядок проведения работ по сертификации продукции, используемой в целях защиты информации от НСД.