МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

Институт дополнительного профессионального образования
и кадрового инжиниринга «Горизонт»

УТВЕРЖДАЮ
Председатель ученого совета,
И.о. ректора ФГБОУ ВО «МГТУ им. Г.И. Носова»
_____ Д.В. Терентьев
«25» января 2023 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА

профессиональной переподготовки

Информационная безопасность.
Техническая защита конфиденциальной информации

Программа утверждена ученым советом МГТУ
Протокол № 2 «25» января 2023 г.

г. Магнитогорск, 2023

1 ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ (АННОТАЦИЯ)

1.1 Цель реализации программы

Цель программы - формирование компетенций, необходимых специалистам, в том числе государственным гражданским служащим и муниципальным служащим, для выполнения нового вида профессиональной деятельности «Информационная безопасность», «Техническая защита информации» в части защиты конфиденциальной информации. подготовка к следующим видам профессиональной деятельности в области информационной безопасности: организационно-управленческая, проектная, эксплуатационная.

Программа реализуется на русском языке.

1.2 Характеристика нового вида профессиональной деятельности и (или) присваиваемой квалификации

Обучающиеся по программе профессиональной переподготовки смогут решать следующие задачи профессиональной деятельности:

1. в организационно-управленческой деятельности:

a. планирование мероприятий, направленных на защиту информации, организация внедрения и применения политик (правил, процедур) по обеспечению информационной безопасности на объектах информатизации;

b. организация мероприятий по контролю (мониторингу) защищенности конфиденциальной информации на объектах информатизации (ОИ);

c. поддержка и совершенствование деятельности по обеспечению информационной безопасности (ИБ) на объектах информатизации (ОИ);

d. проведение аттестационных испытаний и аттестации ОИ по требованиям безопасности информации;

2. в проектной деятельности:

a. определение технических каналов утечки информации (ТКУИ) на ОИ и угроз безопасности информации в автоматизированных и информационных системах;

b. формирование требований к обеспечению ИБ на ОИ (формирование требований к системе защиты информации (СЗИ) ОИ);

c. проведение контроля (мониторинга) защищенности конфиденциальной информации на ОИ, а также анализа применения политик (правил, процедур) по обеспечению ИБ;

d. разработка способов и средств для обеспечения ИБ на ОИ (разработка системы защиты информации объекта информатизации);

e. внедрение способов и средств для обеспечения ИБ на ОИ (внедрение СЗИ ОИ);

f. разработка предложений по совершенствованию организационно-распорядительных документов по безопасности автоматизированных и информационных систем;

3. в эксплуатационной деятельности:

a. установка, монтаж, наладка, испытания, ремонт, техническое обслуживание средств защиты информации;

b. обеспечение ИБ в ходе эксплуатации ОИ;

c. обеспечение ИБ при выводе из эксплуатации ОИ.

1.3 Требования к результатам освоения программы

Программа разработана с учетом требований:

профессионального стандарта: проф. стандарт " Специалист по защите информации в автоматизированных системах ", от 15.09.2016 № 522н;

ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем(уровень специалитета).

(наименование, номер приказа и дата утверждения)

Планируемые результаты обучения

По окончании обучения планируется достижение слушателями следующих результатов по реализации обобщенной трудовой функции: Обслуживание систем защиты информации в автоматизированных системах, 5 уровень квалификации; Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации, 6 уровень квалификации; Внедрение систем защиты информации автоматизированных систем 6 уровень квалификации.

В результате освоения программы у слушателей должны быть сформированы следующие **компетенции**:

Способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защите интересов личности, общества и государства, соблюдать нормы профессиональной этики		
Трудовые действия	*Необходимые умения*	*Необходимые знания*
- Информирование персонала об угрозах безопасности информации. - Информирование персонала о правилах эксплуатации системы защиты автоматизированной системы и отдельных средств защиты информации. - Информирование персонала об ответственности за не санкционированное разглашение различных видов тайн.	- Оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации. - Уметь осуществлять поиск новой методической документации по регламентации мероприятий и оказанию услуг в области защиты информации.	- Нормативные правовые акты в области защиты информации. - Организационные меры по защите информации. - Основы деловой коммуникации. - Методы обработки текстовой и графической информации. - Основы цифровой грамотности.
Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объектов защиты		
Трудовые действия	*Необходимые умения*	*Необходимые знания*
- Ведение протоколов и журналов учета при осуществлении мониторинга систем защиты информации автоматизированных систем. - Ведение протоколов и журналов учета при осуществлении аудита систем защиты информации автоматизированных систем.	- Оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации. - Конфигурировать параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией.	- Понятие угрозы информационной безопасности. - Классификацию угроз информационной безопасности. - Нормативные правовые акты в области защиты информации. - Типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях. - Организационные меры по защите информации. - Особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах. - Технические средства защиты информации. - Методы обработки

		текстовой и графической информации. - Основы цифровой грамотности.
Способность обеспечивать работу систем защиты информации		
Трудовые действия	*Необходимые умения*	*Необходимые знания*
- Проверка работоспособности системы защиты информации автоматизированной системы - Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации - Контроль стабильности характеристик системы защиты информации автоматизированной системы	- Конфигурировать параметры системы защиты информации автоматизированной системы в соответствии с ее эксплуатационной документацией - Обнаруживать и устранять неисправности системы защиты информации автоматизированной системы согласно эксплуатационной документации - Производить монтаж и диагностику компьютерных сетей	- Типовые средства и методы защиты информации в локальных и глобальных вычислительных сетях - Базовая конфигурация системы защиты информации автоматизированной системы - Особенности применения программных и программно-аппаратных средств защиты информации в автоматизированных системах - Типовые средства, методы и протоколы идентификации, аутентификации и авторизации - Нормативные правовые акты в области защиты информации - Организационные меры по защите информации
Способность проводить уудит защищенности информации в автоматизированных системах		
Трудовые действия	*Необходимые умения*	*Необходимые знания*
- Оценка информационных рисков - Обоснование и контроль результатов управленческих решений в области безопасности информации автоматизированных систем - Экспертиза состояния защищенности информации автоматизированных систем - Обоснование критериев эффективности функционирования защищенных автоматизированных систем	- Классифицировать и оценивать угрозы безопасности информации для объекта информатизации - Разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем - Разрабатывать политики безопасности информации автоматизированных систем - Применять инструментальные средства контроля защищенности информации в автоматизированных системах	- Способы защиты информации от "утечки" по техническим каналам - Методы контроля эффективности защиты информации от "утечки" по техническим каналам - Принципы построения систем защиты информации - Нормативные правовые акты в области защиты информации - Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации - Организационные меры по защите информации

1.4. Категория слушателей

К освоению программы допускаются лица, имеющие высшее образование по направлению подготовки (специальности) в области математических и технических наук (в

соответствии с перечнями специальностей и направлений подготовки высшего образования, утвержденными Министерством образования и науки Российской Федерации), подтвержденное документом об образовании.

1.5 Требования к уровню подготовки поступающего на обучение и специальные требования (при наличии)

1.6. Форма обучения

Очная с использованием дистанционных технологий.

1.7. Трудоемкость программы составляет 504 часа.

1.8. Выдаваемый документ

Лицам, успешно освоившим образовательную программу и успешно прошедшим итоговую аттестацию, выдается диплом о профессиональной переподготовке.

2 СОДЕРЖАНИЕ ПРОГРАММЫ

2.1 Учебный план[1)]

Семестр 2)	Наименование дисциплины (модуля)	Трудоемкость, ауд. час.	По учебному плану с использованием дистанционных образовательных технологий, час.								СРС, ауд. час.	Текущий контроль**			Промежуточная аттестация***	
			Аудиторные занятия, ауд.час.*				Дистанционные занятия, ауд.час.									
			всего	из них			всего	из них				РК РГР Реф.	КР	КП	Зачет	Экзамен
				лекц	лаб. раб	прак. зан., семинары		лекц.	лаб. раб	прак. зан., семинары						
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
	1. Организационно-правовые основы технической защиты конфиденциальной информации (ТЗКИ)															
	2. Средства и системы обработки информации															
	3. Способы и средства ТЗКИ от утечки по техническим каналам															
	4. Меры и средства ТЗКИ от не санкционированного доступа (НСД)															
	5. Техническая защита конфиденциальной информации от специальных воздействий															
	6. Организация защиты конфиденциальной информации на ОИ															

	7. Аттестация ОИ по требованиям безопасности информации															
	8. Контроль состояния ТЗКИ															
	9. Безопасность сетей ЭВМ															
	Итого															
	Итоговая аттестация	Итоговый междисциплинарный экзамен														

1) Учебный план может быть совмещен с примерным календарным учебным графиком
2) Даты обучения будут определены при наборе группы на обучение

2.2 Календарный учебный график

Календарный учебный график составляется в форме расписания занятий при наборе группы.

2.3 Рабочие программы дисциплин (модулей)

Информация ограниченного пользования (гриф ДСП)

в) Кадровые условия
Кадровое обеспечение осуществляют:
преподавательский состав из числа докторов, кандидатов наук кафедры информатики и информационных технологий, преподаватели-практики (специалисты организаций) отдела защиты информации ОАО «КредитУралБанк», ООО «ТЕХНАП».

3 ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

Информация ограниченного пользования (гриф ДСП)

4 СОСТАВИТЕЛИ ПРОГРАММЫ

Составители программы:

Баранкова Инна Ильинична - доктор технических наук, доцент, заведующая кафедрой информатики и информационной безопасности.

Михайлова Ульяна Владимировна - кандидат технических наук, доцент, доцент кафедры информатики и информационной безопасности.