Министерство образования и науки Астраханской области

Государственное бюджетное профессиональное образовательное учреждение Астраханской области «Астраханский колледж вычислительной техники»

Согласовано

Зам. директора по УМиВР

_____С.В.Расторгуева

«25» декабря 2020 г.

Утверждаю

Директор колледжа

_____Д.А.Лунев

«25» 12 2020 г.

Дополнительная профессиональная программа

повышения квалификации

Аудит информационной безопасности

Аннотация программы повышения квалификации

Аудит информационной безопасности

Программа дополнительного профессионального образования повышения квалификации разработана с учетом:

Профессионального стандарта «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной зашиты Российской Федерации от 15 сентября 2016 г. №522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный № 43857);

Федерального государственного образовательного стандарта среднего профессионального образования (ФГОС СПО) по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки от 9 декабря 2016 года № 1553 (зарегистрирован Министерством юстиции Российской Федерации 26 декабря 2016 г., регистрационный №44938);

Программа дополнительного профессионального образования повышения квалификации «Аудит информационной безопасности» **предусматривает** использование электронного обучения и дистанционных образовательных технологий.

Организация-разработчик:

Государственное бюджетное профессиональное образовательное учреждение Астраханской области «Астраханский колледж вычислительной техники» (ГБПОУ АО «АКВТ»).

Составители:

Ходжаева Н.Д., преподаватель дисциплин профессионального цикла ГБПОУ АО «АКВТ».

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Нормативно-правовую основу разработки образовательной программы дополнительного профессионального образования – программы повышения квалификации «Аудит информационной безопасности» составляют:

Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

Приказ Министерства образования и науки Российской Федерации от 1 июля 2013 г. № 499 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;

Приказ Министерства образования и науки Российской Федерации от 23.08.2017 № 816 «Об утверждении порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»;

Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. №522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный № 43857);

ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденный приказом Министерства образования и науки от 9 декабря 2016 года № 1553 (зарегистрирован Министерством юстиции Российской Федерации 26 декабря 2016 г., регистрационный №44938).

К освоению дополнительных профессиональных программ допускаются:

- лица, имеющие среднее профессиональное и (или) высшее образование;
- лица, получающие среднее профессиональное и (или) высшее образование.

Документ, выдаваемый после завершения обучения: удостоверение о повышении квалификации.

2. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

2.1. Цель реализации программы

Целью программы

Целью дополнительной профессиональной программы повышения квалификации является совершенствование и актуализация компетенций, обеспечивающих реализацию образовательных программ направления Информационная безопасность.

2.2. Планируемые результаты обучения

Программа направлена на <u>совершенствование</u>:
– профессиональных компетенций

06.033 Специалист по защите информации в автоматизированных системах

Обобщенные трудовые функции в соответствии с профессиональным стандартом		
Обеспечение защиты информации в автоматизированных системах в процессе их эксплуатации		
Трудовая функция: Мониторинг защищенности информации в автоматизированных системах		
Профессиональные компетенции на основании трудовых действий	Необходимые умения	Необходимые знания
Выявление угроз безопасности информации в автоматизированных системах Принятие мер защиты информации при выявлении новых угроз безопасности информации Анализ недостатков в функционировании системы защиты информации автоматизированной системы	Классифицировать и оценивать угрозы информационной безопасности Анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации в автоматизированных системах Применять нормативные документы по противодействию технической разведке Контролировать события безопасности и действия пользователей автоматизированных систем Применять технические средства контроля эффективности мер защиты информации	Содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем Основные угрозы безопасности информации и модели нарушителя в автоматизированных системах Программно-аппаратные средства обеспечения защиты информации автоматизированных систем Методы защиты информации от "утечки" по техническим каналам Нормативные правовые акты в области защиты информации Руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации Организационные меры по защите информации

Трудовая функция: Аудит защищенности информации в автоматизированных системах		
Профессиональные компетенции на основании трудовых действий	Необходимые умения	Необходимые знания
Оценка информационных рисков Обоснование и контроль результатов управленческих решений в области безопасности 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 Применять инструментальные средства контроля защищенности информации в автоматизированных системах	Способы 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

2.3. Объем программы (трудоемкость)
Общая трудоемкость 72 академических часа, из них 72 аудиторных часа.

2.4. Форма обучения
Форма обучения – очная с использованием электронного обучения и дистанционных образовательных технологий.

3. СОДЕРЖАНИЕ ПРОГРАММЫ

3.1. Учебный план и календарный учебный график

Учебный план
программы повышения квалификации
«Аудит информационной безопасности»

Категория слушателей:
К освоению дополнительных профессиональных программ допускаются: лица, имеющие среднее профессиональное и (или) высшее образование; лица, получающие среднее профессиональное и (или) высшее образование.

Срок обучения – 72 часа.
Форма обучения – очная с использованием электронного обучения и дистанционных образовательных технологий

Перечень учебных предметов, курсов, дисциплин (модулей), практик	Трудоемкость, часов				Формы промежуточной аттестации, количество часов
	Всего	В том числе			
		Лекции	Практические занятия	Самостоятельная работа	
Модуль 1. *Обеспечение безопасности межсетевого взаимодействия*	14	12			Семинар, 2
Модуль 2. *Анализ защищенности информационных систем от внешних угроз*	42	12	26		Круглый стол, 4
Модуль 3. *Анализ информационных потоков*	12	4	6		Круглый стол, 2
Практика	-	-	-	-	-
Итоговая аттестация	4				Круглый стол, 4
Итого	72	32	28	-	12

Календарный учебный график

Перечень учебных предметов, курсов, дисциплин (модулей), практик	Учебные недели (дни)/нагрузка в часах					
	1	2	3	4	5	6
Модуль 1. *Обеспечение безопасности межсетевого взаимодействия*	14					
Модуль 2. *Анализ защищенности информационных систем от внешних угроз*		22	20			
Модуль 3. *Анализ информационных потоков*				12		
Итоговая аттестация				4		

3.2. Рабочие программы модулей (курсов)

Модуль 1. ***Обеспечение безопасности межсетевого взаимодействия***

Тема	Количество часов, всего	В том числе практические занятия
Тема 1. Основы сетевого и межсетевого взаимодействия	4	
Тема 2. Аудит информационной безопасности	4	
Тема 3. Механизмы и службы защиты	4	
Промежуточная аттестация	2	2
Итого по модулю 1	**14**	**2**

Тема 1. Основы сетевого и межсетевого взаимодействия
Понятие межсетевого взаимодействия. Уязвимость информационной системы. Угроза информационной системы. Обеспечение информационной безопасности. Политика безопасности. Сетевая политика безопасности.

Тема 2. Аудит информационной безопасности

Понятие аудита. Оценка защищённости технических средств и программного обеспечения. Оценка защищённости сетевой инфраструктуры. Оценка эффективности существующих подсистем информационной безопасности. Анализ бизнес-процессов, нормативной и технической документации. Тест на проникновение. Объекты исследования. Критерии и методики аудита. Результаты аудита информационной безопасности.
Пентест, аудит информационной безопасности и анализ защищённости.

Тема 3. Механизмы и службы защиты
Основные компоненты безопасности: межсетевые экраны, системы обнаружения вторжений, средства контроля целостности, сканеры, средства контроля конфигураций, средства контроля доступа и аутентификации, виртуальные частные сети, встроенные средства безопасности.

Промежуточная аттестация по модулю 1
Семинар «Обзор основных компонентов безопасности», 2 ч.

Модуль 2. ***Анализ защищенности информационных систем от внешних угроз***

Тема	Количество часов, всего	В том числе практические занятия
Тема 1. Вредоносные программы	4	
Тема 2. Удаленные сетевые атаки	4	
Тема 3. Поиск уязвимостей системы	14	10
Тема 4. Обнаружение и предотвращение атак	16	12
Промежуточная аттестация	4	4
Итого по модулю 2	**42**	**26**

Тема 1. Вредоносные программы
Классификация вредоносных программ. Способы и методы заражения системы. Способы и средства защиты от них.

Тема 2. Удаленные сетевые атаки
Характеристика атак. Классификация. Типовой сценарий атаки. Методы атак на информационные системы.

Тема 3. Поиск уязвимостей системы
Сканеры портов. Сканеры уязвимостей. Сетевые анализаторы.

Практическая работа. *Поиск уязвимостей серверов и программ, 6 ч.*

Практическая работа. *Анализ защищенности системы, 6 ч.*

Тема 4. Обнаружение и предотвращение атак
Система обнаружения компьютерных атак (СОА). Система обнаружения вторжений (СОВ). Типовая структура системы обнаружения вторжений. Методы анализа. Требования регуляторов.

Практическая работа. *Обнаружение компьютерных атак, 6 ч.*

Практическая работа. *Обнаружение вторжений, 6 ч.*

Промежуточная аттестация по модулю 2
Круглый стол «Уязвимости современных информационных систем», 4 ч.

Модуль 3. ***Анализ информационных потоков***

Тема	Количество часов, всего	В том числе практические занятия
Тема 1. Анализ информационных потоков и поведенческая аналитика	2	
Тема 2. Применение DLP-систем для защиты от внутренних угроз	8	6
Промежуточная аттестация	2	2
Итого по модулю 4	**12**	**8**

Тема 1. Анализ информационных потоков и поведенческая аналитика.
Данные обрабатываемые в системе (текстовые и графические объекты). Каналы утечки данных. Технологии анализа для защиты цифровых данных компаний

Тема 2. Применение DLP-систем для защиты от внутренних угроз
Возможности и функции DLP-систем. Перехват и анализ сетевого трафика, данных, переданных на внешние устройства, локальные сетевые ресурсы, облачные хранилища, локальные и сетевые принтеры. Контроль и анализ активности пользователя на компьютере, контроль изменений файловых систем компьютеров в режиме реального времени. Контроль утечек и нежелательное распространение конфиденциальной информации через Интернет. Блокировка исходящего сетевого трафика

Практическая работа. *Мониторинг сетевой и компьютерной активности пользователей, 6 ч.*

Промежуточная аттестация по модулю 3
Круглый стол «Обеспечение внутрикорпоративной информационной безопасности», 2 ч.

3.3. Оценочные материалы

Промежуточная аттестация

Модуль 1. Обеспечение безопасности межсетевого взаимодействия
Семинар «Обзор основных компонентов безопасности», 2 ч.

Модуль 2. Анализ защищенности информационных систем от внешних угроз
Круглый стол «Уязвимости современных информационных систем», 4 ч.

Модуль 3. Анализ информационных потоков
Круглый стол «Обеспечение внутрикорпоративной информационной безопасности», 2 ч.

Итоговая аттестация
Итоговая аттестация проводится в форме круглого стола

Тема круглого стола «Аудит информационной безопасности»

Критерии оценки знаний слушателей

В процессе итоговой аттестации слушатель должен продемонстрировать:

- освоение планируемых результатов (знаний, умений, компетенций), предусмотренных программой;
- изучение источников, рекомендованных программой;
- способность самостоятельно пополнять и обновлять знания в ходе дальнейшего обучения и профессиональной деятельности;
- умение выполнять задания с привнесением собственного видения проблемы, собственного варианта решения практической задачи

4. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

4.1. Материально-технические условия реализации программы

мастерские и лаборатории:

- *мастерская «Корпоративная защита от внутренних угроз информационной безопасности»;*
- *лаборатория «Программных и программно-аппаратных средств защиты информации»;*

оборудование:

- *рабочие места на базе вычислительной техники, подключенными к локальной вычислительной сети и информационно-телекоммуникационной сети «Интернет»;*
- *аудиовизуальный комплекс;*
- *средства виртуализации VirtualBox или аналог;*

- *средства обнаружения вторжений и компьютерных атак;*
- *сканеры портов, сканеры уязвимостей, сетевые анализаторы;*
- *DLP-система.*

4.2. Учебно-методическое и информационное обеспечение.

- *Профстандарт: 06.032 Специалист по безопасности компьютерных систем и сетей*
- *Профстандарт: 06.033 Специалист по защите информации в автоматизированных системах*
- *Профстандарт: 06.034 Специалист по технической защите информации*
- *Официальный сайт компании «Код Безопасности» https://www.securitycode.ru/*
- *Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) https://fstec.ru/*
- *Реестр профстандартов https://profstandart-rosmintrud.ru/reestr-profstandartov/*
- *сайт компании «Перспективный мониторинг» https://amonitoring.ru/*
- *сайт компании InfoWatch https://www.infowatch.ru/*

4.3. Кадровое обеспечение программы

Образовательный процесс по модулям обеспечивается педагогическими работниками, имеющими базовое образование, соответствующее профилю модуля, или опыт деятельности в соответствующей профессиональной сфере и систематически занимающимися научно-методической деятельностью.

К образовательному процессу по модулям также могут быть привлечены преподаватели из числа действующих ведущих работников профильных организаций, специалисты и эксперты в области информационной безопасности.