КРАТКАЯ АННОТАЦИЯ ДОПОЛНИТЕЛЬНОЙ ПРОФЕССИОНАЛЬНОЙ ПРОГРАММЫ ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Администрирование информационной безопасности

Общая характеристика компетенций, качественное изменение которых осуществляется в результате обучения

Общепрофессиональные компетенции цифровой экономики:

ОПК-1 - Управление информацией и данными.

Компетенция предполагает способность человека искать нужные источники информации и данные, воспринимать, анализировать, запоминать и передавать информацию с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач.

Профессиональные компетенции цифровой экономики:

ПК-1 – способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций

Под данной компетенцией в рамках настоящей образовательной программы понимается умение обучающегося применять средства защиты, имеющиеся в автоматизированной системе, с целью противодействия угрозам информационной безопасности в соответствии с требованиями нормативных и эксплуатационных документов, а также на основе анализа событий, возникающих в процессе функционирования и способность восстанавливать работоспособность средств защиты при возникновении нештатных ситуаций как техногенного, так и антропогенного характера.

ПК-2 – способность администрировать подсистему информационной безопасности автоматизированной системы.

Под данной компетенцией в рамках настоящей образовательной программы понимается готовность обучающегося выполнять действия по конфигурированию параметров компонентов подсистемы информационной безопасности автоматизированной

системы в соответствии с требованиями нормативных и эксплуатационных документов, а также на основе анализа событий, возникающих в процессе функционирования.

ПК-3 – способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы

Под данной компетенцией в рамках настоящей образовательной программы понимается готовность обучающегося выполнять действия по реализации и корректировке частных политик информационной безопасности, реализуемых в различных подсистемах автоматизированной системы в соответствии с требованиями нормативных и эксплуатационных документов, а также на основе анализа событий, возникающих в процессе функционирования. Выполнять аудит информационной безопасности на основе данных мониторинга событий информационной безопасности.

Описание требований и рекомендаций для обучения по образовательной программе

Обучаемые до начала обучения (сотрудники государственных, муниципальных органов, органов местного самоуправления, организаций различных форм собственности, физические лица, организующие и (или) осуществляющие администрирование информационной безопасности, сотрудники департаментов (отделов, служб) IT и информационной безопасности, специалисты по защите информации) должны знать основы информационных технологий, иметь навыки работы на персональном компьютере под управлением ОС MS Windows, а также иметь навыки работы с антивирусными средствами Лаборатории Касперского.

Для просмотра методических видеоматериалов в режиме «оффлайн», для участия в лекционных и практических занятиях в режиме видеоконференций, а также для самостоятельного выполнения заданий обучаемые должны использовать персональные компьютеры, удовлетворяющие следующим требованиям:

- многоядерный процессор с поддержкой аппаратной виртуализации;
- объем оперативной памяти не менее 8 Гб;
- видеоадаптер с поддержкой HD-видео;
- веб-камера с микрофоном;
- сетевой адаптер, имеющий широкополосное подключение к сети Интернет.

На персональных компьютерах должно быть установлено следующее программное обеспечение:

- браузер с поддержкой просмотра видео (Mozilla Firefox, Google Chrome, MS Edge и т. п. последних версий);
- программа для записи видеоуроков (для преподавателя, например OBS);

– программа просмотра документов в формате PDF;
– программа виртуализации Oracle VirtualBox.

Для выполнения самостоятельных работ обучаемые могут использовать следующие дистрибутивы программных продуктов:

– дистрибутив клиентской операционной системы Windows уровня не ниже Professional и версии не ниже 7 для установки в виртуальную машину;
– дистрибутив серверной операционной системы Windows версии не ниже 2008 R2 для установки в виртуальную машину;
– дистрибутив Kaspersky Security Center для установки в виртуальную машину;
– дистрибутив Kaspersky Endpoint Security для установки в виртуальную машину;

В случае недоступности указанных дистрибутивов обучаемые должны иметь установленную на персональный компьютер операционную систему Windows уровня не ниже Professional и версии не ниже 7 с правами локального администратора.

Краткое описание результатов обучения

В результате освоения программы обучающийся:

должен уметь:

– управлять процессом обеспечения антивирусной безопасности автоматизированных систем для реагирования на инциденты информационной безопасности;
– настраивать права доступа пользователей к объектам при использовании механизмов групп безопасности и наследования прав;
– создавать и редактировать объекты в Microsoft AD; создавать, редактировать групповые политики и управлять ими;
– использовать языки сценариев для автоматизации задач администрирования информационной безопасности;

должен знать:

– архитектуру и основные компоненты средств обеспечения антивирусной безопасности;
– принципы управления антивирусной безопасностью автоматизированной системы;
– механизмы реализации разграничения доступа в файловых системах;
– понятия группы безопасности, отношения доверия и групповой политики;

Знания, умения и навыки, полученные в результате обучения, могут быть востребованы во всех сферах цифровой экономики при выполнении должностных обязанностей по администрированию информационной безопасности.