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» 12 2020 г.

Утверждаю

Директор колледжа

_____Д.А. Лунев

«25» 12 2020 г.

Программа дополнительного образования

«Безопасность компьютерных систем и сетей»

2020

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Нормативно-правовую основу разработки образовательной программы дополнительного образования «Безопасность компьютерных систем и сетей» 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»;

Федеральный государственный образовательный стандарт среднего профессионального образования (ФГОС СПО) по специальности 09.02.06 «Сетевое и системное администрирование», утвержденного приказом Министерства образования и науки от 9 декабря 2016 года № 1548 (зарегистрирован Министерством юстиции Российской Федерации 26 декабря 2016г., регистрационный №44978) (далее – ФГОС СПО);

Профессиональный стандарт 06.026 "Системный администратор информационно-коммуникационных систем", утвержден приказом Министерства труда и социальной защиты Российской Федерации от *5 октября 2015 г. N 684н* (зарегистрирован Министерством юстиции Российской Федерации 18 декабря 2013 г., регистрационный № 30635).

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 дополнительного образования направлена на формирование способности и готовности специалистов к выполнению трудовой функции управление безопасностью сетевых устройств и программного обеспечения и приобретение знаний, умений и навыков по установке специальных средств управления безопасностью сетевых устройств администрируемой сети, настройке параметров управления безопасностью операционных систем сетевых устройств.

2.2. Планируемые результаты обучения

Программа дополнительного профессионального образования повышения квалификации по профессии направлена на совершенствование и (или) формирование у слушателей новой компетенции «Администрирование сетевой подсистемы инфокоммуникационной системы организации»

Программа направлена на <u>совершенствование</u>:

– профессиональных компетенций

Обобщенные трудовые функции в соответствии с профессиональным стандартом *D Администрирование сетевой подсистемы инфокоммуникационной системы организации*		
Трудовая функция : *D/03.6 Управление безопасностью сетевых устройств и программного обеспечения*		
Профессиональные компетенции на основании трудовых действий	Необходимые умения	Необходимые знания
ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.	Определять механизм изменения и модификации базовой конфигурации Внедрять процесс проверки текущей конфигурации на соответствие заданным базовым параметрам (аудит конфигурации) Конфигурировать операционные системы Конфигурировать сетевые устройства Пользоваться нормативно-технической документацией в области	Средства защиты от несанкционированного доступа операционных систем и систем управления базами данных Инструкции по установке администрируемых сетевых устройств Инструкции по эксплуатации администрируемых сетевых устройств Инструкции по установке администрируемого программного обеспечения Инструкции по эксплуатации

	инфокоммуникационных технологий	администрируемого программного обеспечения Защищенные протоколы управления Основные средства криптографии

Программа направлена на приобретение новых профессиональных компетенций, необходимых для выполнения трудовых функций:

Трудовая функция с кодом	Профессиональные компетенции, обеспечивающие выполнение трудовой функции
D/03.6 Управление безопасностью сетевых устройств и программного обеспечения	ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.

2.3. Объем программы (трудоемкость)

Общая трудоемкость 36 академических часа, из них 36 аудиторных часов.

2.4. Форма обучения

Форма обучения – очная

3. СОДЕРЖАНИЕ ПРОГРАММЫ

Учебный план
программы повышения квалификации
«Безопасность компьютерных систем и сетей»

Срок обучения – 36 час.
Форма обучения – очная

Перечень учебных предметов, курсов, дисциплин (модулей), практик	Трудоемкость, часов			Самостоятельная работа студента	Формы аттестации
	Всего	В том числе			
		Лекции	Практические занятия		
Модуль 1	10	6	2		тестирование
Модуль 2	24				тестирование
Итоговая аттестация	2				тестирование
Итого	36				

Календарный учебный график

Наименование модуля/раздела/темы (большой)	Учебные недели (дни)/нагрузка в часах
Модуль 1 Принципы обеспечения безопасности сети	1 нед /10 ч
Тема 1.1 Распространенные угрозы сетевой безопасности	1 нед /2 ч
Практическое занятие 1 Перехват и исследование трафика DNS	1 нед /2 ч
Тема 1.2 Защита от сетевых атак	1 нед /2 ч
Тема 1.3 Управление безопасной сетью	1 нед /2 ч
Тестирование	1 нед /2 ч
Модуль 2. Технологии сетевой безопасности	1 нед - 4 нед /26ч
Тема 2.1 Обеспечение безопасности сетевых устройств	2 нед/2ч
Практическое занятие 2 Настройка параметров безопасности сетевых устройств	2 нед/2ч
Практическое занятие 3 Резервирование маршрутизаторов и коммутаторов	2 нед/2ч
Практическое занятие 4 Отказоустойчивость маршрутизаторов и коммутаторов	2 нед/2ч
Тема 2.2 Аутентификация, авторизация, аудит	2 нед/2ч

Практическое занятие 5 Защита доступа с помощью AAA и протокола RADIUS	3 нед/2ч
Тема 2.3 Реализация технологии межсетевого экрана	3 нед/2ч
Практическое занятие 6 Настройка межстевого экрана на пограничном маршрутизаторе	3 нед/2ч
Тема 2.4 Реализация технологий предотвращения вторжений	3 нед/2ч
Тема 2.5 Принципы работы VPN	3 нед/2ч
Тема 2.6 Компоненты и функционирование IPSec VPN	4 нед/2ч
Практическое занятие 7 Построение туннеля типа Site-to Site VPN	4 нед/2ч
Итоговая аттестация	4 нед/2ч

Рабочие программы модулей

Наименование модулей/разделов/тем курса	**Содержание обучения (по темам в дидактических единицах), наименование и тематика лабораторных/практических работ, учебной практики, используемых образовательных технологий**	**Количество часов**
Раздел 1 Принципы обеспечения безопасности сети		10
Тема 1.1 Распространенные угрозы сетевой безопасности	Векторы сетевых атак. Потеря данных. Злоумышленники и их инструменты. Типы вредоностоного ПО. Обзор различных типов вредоносного ПО. Методы атак. Комплексный подход к защите.	**2**
Практическое занятие 1	**Перехват и исследование трафика DNS**	**2**
Тема 1.2 Защита от сетевых атак	Обзор типов устройств и служб безопасности. Резервное копирование, обновление и установка исправлений.AAA. Межсетевые экраны. Системы предотвращения вторжений (IPS). Устройства защиты электронной почты и веб-трафика	**2**
Тема 1.3 Управление безопасной сетью	Принципы безопасности сетевого дизайна. Безопасная архитектура. Управление процессами и безопасность. Тестирование сети на уязвимости. Непрерывность бизнеса, планирование восстановления аварийных ситуаций. Жизненный цикл сети и планирование, Разработка регламентов компании и политик безопасности	2
Тестирование		**2**
Раздел 2. Технологии сетевой безопасности		26
Тема 2.1 Обеспечение безопасности сетевых устройств	Базовые принципы безопасности. Надежность паролей. Защита паролей. Активация подключения по ssh. Отключение	2

	неиспользуемых служб.	
Практическое занятие 2	**Настройка параметров безопасности сетевых устройств**	2
Практическое занятие 3	**Резервирование маршрутизаторов и коммутаторов**	2
Практическое занятие 4	**Отказоустойчивость маршрутизаторов и коммутаторов**	2
Тема 2.2 Аутентификация, авторизация, аудит	Аутентификация, авторизация и аудит. ACL. Локальная AAA аутентификация. Server-based AAA.	2
Практическое занятие 5	**Защита доступа с помощью AAA и протокола RADIUS**	2
Тема 2.3 Реализация технологии межсетевого экрана	Понятие брандмауэра. Контекстный контроль доступа (CBAC). Политики брандмауэра, основанные на зонах	2
Практическое занятие 6	Настройка зонального экрана на пограничном маршрутизаторе	2
Тема 2.4 Реализация технологий предотвращения вторжений	IPS технологии. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS	2
Тема 2.5 Принципы работы VPN	Виртуальные частные сети и их преимущества. Site-to-Site VPN и VPN для удаленного доступа. VPN для крупных компаний и операторов связи.. Типы VPN.	2
Тема 2.6 Компоненты и функционирование IPSec VPN	IPSec технологии. Компоненты и функционирование IPSec VPN. Инкапсуляция протокола IPSec. Конфиденциальность. Целостность. Аутентификация. Безопасный обмен ключами.	2
Практическое занятие 7	**Построение туннеля типа Site-to Site VPN**	2
Итоговая аттестация		**2**

Оценочные материалы:
Контрольные вопросы, задания, тесты по каждому модулю

Модуль 1

1. Какие меры эффективны в борьбе с киберпреступниками?
   Какие три типа данных киберпреступники чаще всего пытаются похитить у организаций?
2. Что означает термин «уязвимость»?
3. Назовите задачи, которые должна решать комплексная политика безопасности.
4. Каковы три основных принципа кибербезопасности?
5. Назовите три состояния данных.
6. Назовите три вида конфиденциальной информации.
7. Как называют сценарий, при котором злоумышленник отправляет мошенническое электронное сообщение, выдавая его за сообщение из надежного источника?
8. Злоумышленник находится около магазина и с помощью беспроводной связи копирует адреса электронной почты и списки контактов с устройств ничего не подозревающих прохожих. К какому типу относится такая атака?
9. Как называют атаку, при которой электронное сообщение адресуется конкретному сотруднику финансового учреждения?
10. Что означает термин «логическая бомба»?
11. Как называют программу или код для обхода стандартного механизма аутентификации?
12. Что именно модифицируют руткиты?
13. Что происходит на компьютере, если объем данных превышает пределы буфера?
14. Пользователь видит на экране сообщение о том, что доступ к данным закрыт и будет восстановлен только после уплаты некоторой денежной суммы. К какой категории относится вредоносное ПО, выводящее такие сообщения?
15. К какому типу относятся атаки, при которых для доступа к базе данных SQL используется поле, в которое пользователь обычно вводит информацию?
16. Как называется ПО, которое демонстрирует всплывающие окна с рекламой, тем самым принося доход его авторам?
17. Чем вирусы отличаются от интернет-червей?
18. Как называется уязвимость, посредством которой злоумышленники внедряют сценарии в веб-страницы, просматриваемые пользователями?
19. Назовите два основных признака спам-письма.
20. Как называют атаку, при которой злоумышленник отправляет короткое SMS-сообщение, обманом вынуждающее жертву посетить веб-сайт?
    При какой атаке цель выводится из строя путем отправки ей огромного количества запросов от множества других систем?
    При какой атаке компьютер выводится из строя за счет переполнения памяти или перегрузки центрального процессора?
21. Назовите две тактики социальной инженерии, применяемые для получения персональных данных от ничего не подозревающей жертвы?
22. Злоумышленник применяет специальное ПО, чтобы получить информацию о компьютере пользователя. К какой категории относится такое ПО?
23. Какой механизм можно применить в организации в качестве средства защиты от непреднамеренного изменения информации авторизованными пользователями?
24. Какой из принципов подразумевает исключение доступа неавторизованных лиц, ресурсов и процессов к информации?

Модуль 2

1. Перечислите базовые принципы безопасности.
2. Опишите принципы выбора надежных паролей.
3. Перечислите способы защиты паролей.
4. Как осуществляется активация подключения по ssh.
5. Как можно отключить неиспользуемые службы.
6. Дайте определение понятиям аутентификация, авторизация и аудит.
7. Назначение и настройка списков доступа ACL.
8. Понятие локальной AAA аутентификации.
9. Понятие Server-based AAA.
10. Понятие брандмауэра.
11. Контекстный контроль доступа (CBAC).
12. Политики брандмауэра, основанные на зонах
13. IPS технологии.
14. IPS сигнатуры.
15. Реализация IPS.
16. Проверка и мониторинг IPS
17. Виртуальные частные сети и их преимущества.
18. Site-to-Site VPN и VPN для удаленного доступа.
19. VPN для крупных компаний и операторов связи.
20. Типы VPN.
21. IPSec технологии.
22. Компоненты и функционирование IPSec VPN.
23. Инкапсуляция протокола IPSec.
24. Конфиденциальность. Целостность. Аутентификация.
25. Безопасный обмен ключами.
26. Как называется защищенная виртуальная сеть, существующая внутри общедоступной сети?
27. Назовите два метода обеспечения доступности систем.
28. Назовите три метода идентификации, применяемые в процессе аутентификации.
29. Назовите два метода проверки целостности данных.
30. Назовите два метода обеспечения конфиденциальности.
31. Соотнесите описание с типом фильтрации брандмауэра.
32. Какова цель функции проверки подлинности?
33. Какая функция межсетевого экрана контролирует, чтобы поступающие в сеть пакеты были легитимными ответами на запросы внутренних узлов?
34. Какая команда поможет смягчить атаки паролей грубой силы против маршрутизатора?
35. Какая функция SSH делает его более безопасным, чем Telnet для управлением устройствами?
36. В чем заключается преимущество использования SSH по сравнению с Telnet?
37. В чем состоит роль IPS?
38. Пользователь реорганизует сеть небольшой компании и намерен обеспечить безопасность, не выходя за рамки небольшого бюджета. Между сетью компании и сетью интернет-провайдера пользователь помещает новый межсетевой экран, который снабжен системой обнаружения вторжений и функционирует с учетом особенностей используемого программного обеспечения. Кроме того, пользователь отделяет сеть компании от общедоступной сети с помощью второго межсетевого экрана. При этом во внутренней сети компании пользователь развертывает систему предотвращения вторжений IPS. Какой подход применяется в данном случае?
39. Дайте точное определение понятию резервирование.

40. Сетевой администратор обновляет сеть малого предприятия, чтобы уделять приоритетное внимание трафику приложений в реальном времени. Какие два типа сетевых служб пытается реализовать администратор сети?
41. Какова цель небольшой компании, использующей утилиту анализатора протоколов для захвата сетевого трафика в сегментах сети, где компания рассматривает возможность обновления сети?
42. Сетевой инженер анализирует отчеты по недавно проведенной проверке базового уровня сети. Какие показатели будут свидетельствовать о возможной проблеме с задержками в сети?
43. Для чего сетевой администратор может использовать служебную программу tracert ?
44. Какой способ считается наиболее эффективным для минимизации последствий атаки вируса-червя?
45. Инженер должен задокументировать текущие настройки всех сетевых устройств в колледже, включая устройства, расположенные на прилегающих территориях. Какой протокол лучше всего использовать для защищенного доступа к сетевым устройствам?
46. Администратор решает использовать "12345678!" в качестве пароля для вновь установленного маршрутизатора. Что можно сказать о выбранном пароле?
47. Администратор решает использовать «admin» в качестве пароля для вновь установленного маршрутизатора. Что можно сказать о выбранном пароле?
48. Сетевой специалист устраняет неполадки и должен проверить IP-адреса всех интерфейсов на маршрутизаторе. Какую команду лучше использовать?
49. Студенты, подключенные к одному и тому же коммутатору, работают медленнее чем обычно. Администратор подозревает проблему настройки дуплекса. Какую команду лучше всего использовать для выполнения задачи?
50. Пользователь хочет знать IP-адрес ПК. Какую команду лучше всего использовать для выполнения задачи?
51. Студент хочет сохранить конфигурацию маршрутизатора в NVRAM. Какую команду лучше всего использовать для выполнения задачи?
52. Специалист по поддержке должен знать IP-адрес беспроводного интерфейса на MAC. Что является наилучшей командой для выполнения задачи?
53. Сетевой техник устраняет неполадки и должен проверить все адреса интерфейса IPv6 на маршрутизаторе. Что является наилучшей командой для выполнения задачи?
54. Учитель испытывает трудности с подключением своего компьютера к сети класса. Он должен убедиться, что шлюз по умолчанию настроен правильно. Что является наилучшей командой для выполнения задачи?
55. Только сотрудники, подключенные к интерфейсам IPv6, испытывают трудности с подключением к удаленным сетям. Аналитик хочет проверить, включена ли маршрутизация IPv6. Что является наилучшей командой для выполнения задачи?
56. Администратор решает проблемы подключения и должен определить IP-адрес веб-сайта. Что является наилучшей командой для выполнения задачи?
57. Только сотрудники, подключенные к интерфейсам IPv6, испытывают трудности с подключением к удаленным сетям. Аналитик хочет проверить, включена ли маршрутизация IPv6. Что является наилучшей командой для выполнения задачи?
58. Политика корпоративной безопасности требует, чтобы трафик от клиентов с удаленным доступом VPN был разделен между надежным трафиком, предназначенным для корпоративных подсетей, и ненадежным трафиком, предназначенным для публичного Интернета. Какое VPN-решение должно быть реализовано для обеспечения соблюдения корпоративной политики?

59. Что согласовывается при создании туннеля IPsec между двумя хостами IPsec во время фазы IKE 1?
60. В чем преимущество использования брандмауэра фильтрации пакетов по сравнению с высококачественной системой брандмауэра?
61. В каком утверждении верно определена характеристика протокола IKE?
62. На какие три действия может быть настроен IPS брандмауэра Cisco IOS при обнаружении вторжения? (Выберите три варианта)
63. Какие два протокола можно выбрать с помощью Cisco AnyConnect VPN Wizard для защиты трафика внутри VPN-тунпеля?
64. Сопоставьте метод тестирования сетевой безопасности с тем, как он используется для проверки сетевой безопасности.
65. В каком заявлении описывается использование классов сертификатов в PKI?
66. Выберите безопасный вариант конфигурации для удаленного подключения к сетевому устройству?
67. Специалист по безопасности оценивает новое предложение по обеспечению безопасности операций, направленное на ограничение доступа ко всем серверам. В чем преимущество использования тестирования сетевой безопасности для оценки нового предложения?
68. Какое средство обеспечения безопасности обеспечит защиту от несанкционированного управления сетевым устройством?

4 ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

4.1 Материально-технические условия реализации программы

Для обучения слушателей программы используется оборудование мастерской «Сетевое и системное администрирование»:

Техническое и программное обеспечение:

– персональный компьютер в сборке (системный блок Aquarius Pro W60 K12 (Intel Core i7, 8700/16 GB DDr4/SSD 240 GB/Win 10 Pro);

– монитор – 2 шт., AOC Professional 12490VXQ/BT (23.8", 75 Гц, IPS 1920x1080, 16:9, 250 кд/м^2, (GTG) 5 мс, HDMI, Display Port);

– интерактивный комплекс: панель 65" EdFlat ED65I (Type-C) со встроенным компьютером EdFlatOP3P;

– коммутационное оборудование;

– Система для проведения образовательных видеоконференций (IP-камера);

Программное обеспечение:

– операционные системы Windows, UNIX;

– пакет офисных программ;

– пакет САПР;

– серверная ОС Windows Server 2012 или более новая версия;

– лицензионные антивирусные программы;

– лицензионные программы восстановления данных;

– лицензионные программы по виртуализации.

Для лиц с ограниченными возможностями здоровья созданы специальные условия.

4.2 Учебно-методическое и информационное обеспечение

– Раздаточные материалы для слушателей.

– Отраслевые и другие нормативные документы.

– Электронные ресурсы

4.3 Кадровое обеспечение программы

Количество преподавателей, привлеченных для реализации программы 1.

№ п/п	ФИО	Статус в экспертном сообществе Ворлдскиллс с указанием компетенции	наименование организации
1	Бойченко Людмила Михайловна	Преподаватель дисциплин общепрофессионального цикла и профессиональных модулей	ГБПОУ АО «Астраханский колледж вычислительной техники»,