Министерство образования и науки Астраханской области

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

Согласовано
Зам. директора по УМ и ВР
_____С.В. Расторгуева
«25» 12 20 20 г.

Утверждаю
Директор колледжа
_____Д.А. Лунев
«24» 12 20 20 г.

Дополнительная профессиональная программа

повышения квалификации

«Введение в кибербезопасность»

Аннотация программы повышения квалификации

Введение в кибербезопасность

Программа дополнительного профессионального образования разработана на основе:

Профессионального стандарта 06.026 "Системный администратор информационно-коммуникационных систем", утвержденного приказом Министерства труда и социальной защиты Российской Федерации от *5 октября 2015 г. № 684н* (зарегистрирован Министерством юстиции Российской Федерации 19 октября 2015 г., регистрационный № 39361);

Федерального государственного образовательного стандарта 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).

Рабочая программа дополнительного профессионального образования «Введение в кибербезопасность» не 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:

Бойченко Л.М., преподаватель дисциплин профессионального цикла ГБПОУ АО «АКВТ».

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Нормативно-правовую основу разработки образовательной программы дополнительного профессионального образования – программы повышения квалификации «Введение в кибербезопасность» 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 юстнции 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 повышения квалификации является формирование способности и готовности специалистов к выполнению трудовой функции управление безопасностью сетевых устройств и программного обеспечения и приобретение знаний, умений и навыков по настройке параметров управления безопасностью операционных систем сетевых устройств, установке специальных средств управления безопасностью сетевых устройств администрируемой сети, установке и настройке средств обеспечения безопасности удаленного доступа

2.2. Планируемые результаты обучения

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

Программа направлена на совершенствование следующих 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 инфокоммуникационных технологий	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 администрируемого программного обеспечения Защищенные протоколы управления Основные средства криптографии

2.3. Объем программы (трудоемкость)

Общая трудоемкость 24 академических часа.

2.4. Форма обучения .Форма обучения – очная

3. СОДЕРЖАНИЕ ПРОГРАММЫ

3.1 Учебный план и календарный учебный график

Учебный план
программы повышения квалификации
«Введение в кибербезопасность»

Категория слушателей: лица имеющие или получающие среднее профессиональное и (или) высшее образование.
Срок обучения – 24 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 Основы кибербезопасности	6	4	2		Тестирование
Модуль 2 Методы киберзащиты	16	6	10		
Итоговая аттестация	2				Экзамен
Итого	24				

Календарный учебный график

Перечень учебных предметов, курсов, дисциплин (модулей), практик	**Учебные недели/нагрузка в часах**				
	1	**2**	**3**	**4**	**5**
Модуль 1 Основы кибербезопасности	6				
Модуль 2 Методы киберзащиты	6	10			
Итоговая аттестация		2			

3.2 Рабочие программы модулей

Модуль 1. Основы кибербезопасности

Тема	Количество часов, всего	Из них практические занятия
Тема 1 Угрозы, уязвимости и атаки	4	2
Тема 2 Основополагающие принципы киберзащиты	1	
Тестирование	1	

Тема 1. Угрозы, уязвимости и атаки
Уровни обеспечения кибербезопасности. Распространение киберугроз. Типовые угрозы. Вредоносное ПО. Атаки через браузер и электронную почту и защита от них. Социальная инженерия. Методы обмана. Защита от обмана. Кибератаки. Атаки на беспроводные сети и мобильные устройства и защита от них. Атаки на приложения.

Тема 2 Основополагающие принципы киберзащиты
Принципы информационной безопасности: конфиденциальность, целостность и доступность. Цели защиты киберпространства. Типы конфиденциальной информации. Проблема защиты данных. Навыки и знания, необходимые для обеспечения защиты. Законодательная база. Модель кибербезопасности.

Практическая работа 1. Обнаружение угроз и уязвимостей

Модуль 2. Методы киберзащиты

Тема	Количество часов, всего	Из них практические занятия
Тема 1 Способы защиты данных	8	6
Тема 2 Повышение доступности и аварийное восстановление	4	2
Тема 3 Реагирование на инциденты	4	2
Итоговая аттестация	2	

Тема 1. Способы защиты данных
Управление доступом. Требования к целостности данных. Проверка целостности. Системы хранения данных. Защита передаваемых и обрабатываемых данных. Программные и аппаратные меры защиты. Средства защиты на базе облака. Политики безопасности.

Практическая работа 2. Аутентификация и разграничение доступа

Практическая работа 3. Обеспечение секретности и целостности

Практическая работа 4. Применение электронной цифровой подписи

Тема 2 Повышение доступности и аварийное восстановление
Принципы проектирования систем высокой доступности. Asset Management. Многоуровневая защита. Резервирование. Обеспечение отказоустойчивости. Аварийное восстановление.

Практическая работа 5. Применение средств резервирования

Тема 3. Реагирование на инциденты
Этапы реагирования на инциденты. Технология реагирования на инциденты. Средства анализа угроз. Системы обнаружения и предотвращения вторжений.

Практическая работа 6. Использование средств аудита

3.3 Оценочные материалы:

Промежуточная аттестация по программе предназначена для оценки освоения слушателем модулей программы и проводится в виде зачетов по итогам выполненных практических заданий. По результатам промежуточных испытаний в форме зачётов выставляются отметки «зачтено» или «не зачтено».

Итоговая аттестация проходит в форме аттестационного испытания практико-ориентированного характера.

По модулю 1 промежуточная аттестация проводится в форме тестирования. Примерные вопросы для подготовки к тестированию приведены ниже.

По модулю 2 промежуточная аттестация проходит в форме зачета выполненных практических работ.

Модуль 1. Примерные вопросы для подготовки к тестированию.

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?

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	Бойчепко Людмила Михайловна	Преподаватель дисциплин общепрофессионального цикла и профессиональных модулей	ГБПОУ АО «Астраханский колледж вычислительной техники»,