

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

 А.А.Лунев

«25» 12 2020 г.



Дополнительная профессиональная программа

повышения квалификации

Обеспечение безопасного функционирования сайтов

**Аннотация программы повышения квалификации  
Обеспечение безопасного функционирования сайтов**

Программа дополнительного профессионального образования повышения квалификации по профессии разработана на основе:

Профессионального стандарта Системный администратор информационно-коммуникационных систем, утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 05 октября 2015г. №684н (зарегистрирован Министерством юстиции Российской Федерации 19 октября 2015г., регистрационный № 39361);

Рабочая программа дополнительного профессионального образования повышения квалификации «Обеспечение безопасного функционирования сайтов» 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:

Коцарева А.А., преподаватель дисциплин профессионального цикла ГБПОУ АО «АКВТ».

## 1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Нормативно-правовую основу разработки образовательной программы дополнительного профессионального образования – программы повышения квалификации «Обеспечение безопасного функционирования сайтов» 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 «Системный администратор информационно-коммуникационных систем», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 05 октября 2015г. № 684н (зарегистрирован Министерством юстиции Российской Федерации 19 октября 2015г., регистрационный № 39361);

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 является повышение квалификации слушателей в результате освоения программы «Обеспечение безопасного функционирования сайтов».

В результате освоения программы повышения квалификации, слушатель должен Уметь:

- проверять корректность данных, вводимых пользователями;
- применять понятие безопасности приложений и классификация опасности;
- осуществлять аудит безопасности веб-сайтов и веб-приложений в соответствии

с регламентами по безопасности.

Знать:

- основные принципы построения безопасных сайтов;
- источники угроз информационной безопасности и меры по их предотвращению;
- регламенты и методы разработки безопасных веб-сайтов и веб-приложений;
- методы шифрования.

### 2.2. Планируемые результаты обучения

**Программа направлена на совершенствование:**

– профессиональных компетенций

Устанавливать аппаратно-программные средства защиты прикладного программного обеспечения

Настраивать аппаратно-программные средства защиты прикладного программного обеспечения

Проводить регламент обеспечения защиты информации в соответствии с политикой информационной безопасности

Проводить регламент обеспечения защиты информационных систем в соответствии с политикой информационной безопасности (в том числе управление правами доступа)

|                                                                                                                                                                                   |                                                                                                                               |                                                                                                             |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Обобщенные трудовые функции в соответствии с профессиональным стандартом<br>В Администрирование прикладного программного обеспечения инфокоммуникационной<br>системой организации |                                                                                                                               |                                                                                                             |
| Трудовая функция : В / 05.5 Реализация регламентов обеспечения информационной<br>безопасности прикладного программного обеспечения                                                |                                                                                                                               |                                                                                                             |
| Профессиональные<br>компетенции на основании<br>трудовых действий                                                                                                                 | Необходимые умения                                                                                                            | Необходимые знания                                                                                          |
| Установка аппаратно-<br>программных средств<br>защиты прикладного<br>программного обеспечения<br>Настройка аппаратно-                                                             | Выполнять настройку<br>прикладного программного<br>обеспечения в соответствии<br>с регламентами обеспечения<br>информационной | Основы обеспечения<br>информационной<br>безопасности<br>Локальные правовые акты в<br>области информационной |

|                                                                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>программных средств защиты прикладного программного обеспечения</p> <p>Проведение регламентов обеспечения защиты информации в соответствии с политикой информационной безопасности</p> <p>Проведение регламентов обеспечения защиты информационных систем в соответствии с политикой информационной безопасности (в том числе управление правами доступа)</p> | <p>безопасности</p> <p>Производить авторизацию пользователей прикладного программного обеспечения</p> <p>Применять программно-аппаратные средства защиты информации</p> <p>Применять программные средства защиты информации</p> | <p>безопасности, действующие в организации</p> <p>Типовые уязвимости, учитываемые при настройке устанавливаемого программного обеспечения</p> <p>Типовые уязвимости, учитываемые при эксплуатации устанавливаемого программного обеспечения</p> <p>Методы и средства защиты информации</p> <p>Регламенты проведения профилактических работ на администрируемой инфокоммуникационной системе</p> <p>Регламенты обеспечения информационной безопасности</p> <p>Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы</p> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

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

| Трудовая функция с кодом                                                                                     | Профессиональные компетенции, обеспечивающие выполнение трудовой функции                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| В / 05.5 Реализация регламентов обеспечения информационной безопасности прикладного программного обеспечения | <p>Установка аппаратно-программных средств защиты прикладного программного обеспечения</p> <p>Настройка аппаратно-программных средств защиты прикладного программного обеспечения</p> <p>Проведение регламентов обеспечения защиты информации в соответствии с политикой информационной безопасности</p> <p>Проведение регламентов обеспечения защиты информационных систем в соответствии с политикой информационной безопасности (в том числе управление правами доступа)</p> |

### **2.3. Объем программы (трудоемкость)**

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

### **2.4. Форма обучения**

Форма обучения – очная, заочная с использованием электронного обучения и дистанционных образовательных технологий

### 3. СОДЕРЖАНИЕ ПРОГРАММЫ

#### 3.1. Учебный план и календарный учебный график

**Учебный план**  
программы повышения квалификации  
«Обеспечение безопасного функционирования сайтов»

Категория слушателей:

Срок обучения – 36 час.

Форма обучения – очная, заочная с использованием электронного обучения и дистанционных образовательных технологий

| Перечень учебных предметов, курсов, дисциплин (модулей), практик          | Трудоемкость, часов |             |                      |                        | Формы аттестации              |
|---------------------------------------------------------------------------|---------------------|-------------|----------------------|------------------------|-------------------------------|
|                                                                           | Всего               | В том числе |                      |                        |                               |
|                                                                           |                     | Лекции      | Практические занятия | Самостоятельная работа |                               |
| Модуль 1. Технологии обеспечения безопасности веб-сайтов и веб-приложений | 34                  | 10          | 22                   | -                      | Тестирование, 2ч              |
| Итоговая аттестация                                                       | 2                   | -           | -                    | -                      | Защита практических работ, 2ч |
| Итого                                                                     | 36                  | 10          | 22                   | -                      | 4                             |

#### Календарный учебный график

| Перечень учебных предметов, курсов, дисциплин (модулей), практик          | Учебные недели (дни)/нагрузка в часах |    |   |   |   |   |
|---------------------------------------------------------------------------|---------------------------------------|----|---|---|---|---|
|                                                                           | 1                                     | 2  | 3 | 4 | 5 | 6 |
| Модуль 1. Технологии обеспечения безопасности веб-сайтов и веб-приложений | 24                                    | 10 |   |   |   |   |
| Итоговая аттестация                                                       |                                       | 2  |   |   |   |   |

#### 3.2. Рабочие программы модулей (курсов)

##### Модуль 1. Технологии обеспечения безопасности веб-сайтов и веб-приложений

| Тема                                             | Количество часов, всего | В том числе практические занятия |
|--------------------------------------------------|-------------------------|----------------------------------|
| Основы построения безопасных сайтов              | 2                       |                                  |
| Угрозы информационной безопасности               | 6                       | 4                                |
| Разработка безопасных веб-приложений             | 4                       | 2                                |
| Безопасность персональных данных                 | 10                      | 8                                |
| Корректность вводимых данных. Методы шифрования. | 10                      | 8                                |
| Промежуточная аттестация (тестирование)          | 2                       |                                  |
| Итоговая аттестация (защита практических работ)  | 2                       |                                  |

**Тема 1. Основы построения безопасных сайтов.**

Основные принципы построения безопасных сайтов. Понятие безопасности приложений и классификация опасностей.

**Тема 2.** Угрозы информационной безопасности.

Источники угроз информационной безопасности и меры по их предотвращению.

**Практическая работа № 1.** Сбор информации о web-приложениях (4ч)

**Тема 3.** Разработка безопасных веб-приложений.

Регламенты и методы разработки безопасных веб-приложений.

**Практическая работа №2.** Внутренняя и внешняя поисковая оптимизация (SEO)

(2ч)

**Тема 4.** Безопасность персональных данных.

Безопасная аутентификация и авторизация. Повышение привилегий и общая отказоустойчивость системы.

**Практическая работа №3.** Тестирование защищенности механизма управления доступом и сессиями. (4ч)

**Практическая работа №4.** Тестирование на устойчивость к атакам отказа в обслуживании. (4ч)

**Тема 5.** Корректность вводимых данных. Методы шифрования..

Проверка корректности данных, вводимых пользователем. Публикация изображений и файлов. Методы шифрования. SQL- инъекции. XSS-инъекции.

**Практическая работа №5.** Поиск уязвимостей к атакам XSS. (4ч)

**Практическая работа №6.** Поиск уязвимостей к атакам SQL-injection. (4ч)

### 3.3. Оценочные материалы

**Промежуточная аттестация** по окончании изучения Модуля 1 проводится в форме тестирования, состоящего из 25 вопросов.

Типовые вопросы:

*1 Основными источниками угроз информационной безопасности являются все указанное в списке:*

- a) Хищение жестких дисков, подключение к сети, инсайдерство*
- b) Перехват данных, хищение данных, изменение архитектуры системы*



- c) Хищение данных, подкуп системных администраторов, нарушение регламента работы

## **2 Виды информационной безопасности:**

- a) Персональная, корпоративная, государственная
- b) Клиентская, серверная, сетевая
- c) Локальная, глобальная, смешанная

## **3 Цели информационной безопасности – своевременное обнаружение, предупреждение:**

- a) несанкционированного доступа, воздействия в сети
- b) инсайдерства в организации
- c) чрезвычайных ситуаций

## **4 Основные объекты информационной безопасности:**

- a) Компьютерные сети, базы данных
- b) Информационные системы, психологическое состояние пользователей
- c) Бизнес-ориентированные, коммерческие системы

## **5 Основными рисками информационной безопасности являются:**

- a) Искажение, уменьшение объема, перекодировка информации
- b) Техническое вмешательство, выведение из строя оборудования сети
- c) Потеря, искажение, утечка информации

.....

## **Итоговая аттестация**

Итоговая аттестация проводится в форме защиты практических работ.

## **Критерии оценки знаний слушателей**

В процессе итоговой аттестации слушатель должен продемонстрировать:

В ходе выполнения и защиты практических работ умения:

- проверять корректность данных, вводимых пользователями;
- применениис понятия безопасности приложений и классификации опасности;
- осуществлять аудит безопасности веб-приложения в соответствии с регламентами по безопасности;

знания:

- основных принципов построения безопасных сайтов;
- источников угроз информационной безопасности и мер по их предотвращению;
- регламентов и методов разработки безопасных веб-приложений;
- основных методов шифрования.

## **4. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ**

## 4. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

### 4.1. Учебно-методическое и информационное обеспечение.

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы.

#### 4.2.1. Основная литература

1. Ю. Родичева «Нормативная база и стандарты в области информационной безопасности»: учеб. пособие для студ. с ред. проф. образования / А.В. Остроух. – 1-е изд. – М.: Издательский центр «Академия», 2015. – 208 с.

2. А.А. Борисенко Web-дизайн. Просто как дважды два. -: Экспо, 2017 - 320с.

3. К. Панфилов. По ту сторону веб-страницы. – СПб, 2015. – 440с.

4. Е.В. Михеева Информационные технологии в профессиональной деятельности: учеб. пособие для студ. с ред. проф. образования / Е.В.Михеева. – 12-е изд., стер. – М.: Издательский центр «Академия», 2016. – 384 с.

5. Е.В. Михеева Практикум по информационным технологиям в профессиональной деятельности: учеб. пособие для студ. учреждений с ред. проф. образования / Е.В.

Михеева. – 12-е изд., стер. – М.: Издательский центр «Академия», 2016. – 256 с.

#### 4.2.2. Дополнительная литература

1. И.А. Коноплева, О.А. Хохлова, А.В. Денисов Информационные технологии: учебное пособие / под ред. И.А.Коноплевой. – 2-е изд., перераб. и доп. – М.: Проспект, 2010. – 328с.

2. Д.Ю. Усенков Коммуникационные технологии: практикум / Д.Ю. Усенков, О.Б. Богомолова. – М.: БИНОМ. Лаборатория знаний, 2013. – 303 с.: ил.

#### 4.2.3. Интернет-ресурсы

1. <http://claw.ru/> - Образовательный портал

2. <http://ru.wikipedia.org/> - Свободная энциклопедия

3. <http://intuit.ru>

### 4.2.Кадровое обеспечение программы

Количество ППС (физических лиц), привлеченных для реализации программы 1 чел. Из них:

Экспертов с правом оценки демонстрационного экзамена по стандартам Ворлдскиллс 1 чел.

| № п/п | ФИО                              | Статус в экспертном сообществе Ворлдскиллс с указанием компетенции                                                      | Должность, наименование организации                                   |
|-------|----------------------------------|-------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
|       | Коцарева Анастасия Александровна | Эксперт с правом оценки демонстрационного экзамена по стандартам Ворлдскиллс по компетенции «Веб – дизайн и разработка» | Преподаватель, ГБПОУ АО «Астраханский колледж вычислительной техники» |