**Паспорт Образовательной программы**

**«**Основы безопасной веб-разработки**»**

|  |  |
| --- | --- |
| Версия программы | 2 |
| Дата Версии | 23.10.2020 |

1. **Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | Автономная некоммерческая организация инновационного развития образования и науки «ФИРОН» |
| 1.2 | Логотип образовательной организации |  |
| 1.3 | Провайдер ИНН | 6167136916 |
| 1.4 | Ответственный за программу ФИО | Гвоздева Вера Сергеевна |
| 1.5 | Ответственный должность | Комьюнити-менеджер |
| 1.6 | Ответственный Телефон | +7 (928) 605-80-15 |
| 1.7 | Ответственный Е-mail | v.gvozdeva@firon.org |

1. **Основные Данные**

|  |  |  |
| --- | --- | --- |
| № | Название | Описание |
| 2.1 | Название программы | «Основы безопасной веб-разработки» |
| 2.2 | Ссылка на страницу программы | <https://edu.firon.org/mod/forum/discuss.php?d=7> |
| 2.3 | Формат обучения | Онлайн |
|  | Подтверждение от ОО наличия возможности реализации образовательной программы с применением электронного обучения и (или) дистанционных образовательных технологий с возможностью передачи данных в форме элементов цифрового следа | У ОО имеется собственная электронная платформа для реализации образовательной программы с применением электронного обучения и (или) дистанционных образовательных технологий с возможностью передачи данных в форме элементов цифрового следа - <https://edu.firon.org/> |
| 2.4 | Уровень сложности | Базовый |
| 2.5 | Количество академических часов | 72 |
|  | Практикоориентированный характер образовательной программы: не менее 50 % трудоёмкости учебной деятельности отведено практическим занятиям и (или) выполнению практических заданий в режиме самостоятельной работы (кол-во академических часов) | 57 часов (79,1%) |
| 2.6 | Стоимость обучения одного обучающегося по образовательной программе, а также предоставление ссылок на 3 (три) аналогичные образовательные программы иных организаций, осуществляющих обучение, для оценки объективности стоимости или обоснование уникальности представленной образовательной программы в случае отсутствия аналогичных образовательных программ на рынке образовательных услуг | 30 000  1. <https://loftschool.com/course/web-beginner/>  2. <https://otus.ru/lessons/security-web-dev/>  3. <https://www.academyit.ru/courses/%D0%98%D0%91512/> |
| 2.7 | Минимальное количество человек на курсе | 10 |
| 2.8 | Максимальное количество человек на курсе | 1000 |
| 2.9 | Данные о количестве слушателей, ранее успешно прошедших обучение по образовательной программе | Данная программа реализуется впервые |
| 2.10 | Формы аттестации | тестирование |
|  | Указание на область реализации компетенций цифровой экономики, к которой в большей степени относится образовательная программа, в соответствии с Перечнем областей | Программирование и создание ИТ-продуктов |

1. **Аннотация программы**

Дополнительная профессиональная программа повышения квалификации «Основы безопасной веб-разработки» (далее – программа) предназначена для повышения квалификации лиц, имеющих среднее или высшее профессиональное образование.

Программа построена с учетом характеристики профессиональной деятельности специалиста в сфере веб-разработки, определяющей область и объекты профессиональной деятельности, виды деятельности и соответствующие им профессиональные задачи.

Настоящая программа составлена на основе следующих нормативно-правовых документов:

* Федеральный закон от 29 декабря 2012 г. №273-ФЗ «Об образовании в Российской Федерации»;
* Приказ Министерства образования и науки Российской Федерации (Минобрнауки России) от 1 июля 2013 г. N 499 г. Москва «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам» (зарегистрирован Министерством юстиции Российской Федерации 20 августа 2013 г., регистрационный № 29444);
* Приказ Министерства труда Российской федерации (Минтруда России) от 12 апреля 2013г. №148н «Об утверждении уровней квалификации в целях разработки проектов профессиональных стандартов»; - Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 09.02.07 Информационные системы и программирование (утв. приказом Министерства образования и науки РФ от 9 декабря 2016 г. № 1547);
* Приказ Минтруда России от 18.01.2017 № 44н «Об утверждении профессионального стандарта «Разработчик Web и мультимедийных приложений» (зарегистрирован Министерством юстиции Российской Федерации 31 января 2017 г., регистрационный № 45481)
* Методические рекомендации по организации итоговой аттестации при реализации дополнительных профессиональных программ (письмо Минобрнауки России от 30.03.2015 N АК-821/06 «О направлении методических рекомендаций по итоговой аттестации слушателей»);
* Методические рекомендации по разработке основных профессиональных образовательных программ и дополнительных профессиональных программ с учетом соответствующих профессиональных стандартов (утверждены Министром образования и науки Российской Федерации от 22 января 2015г. №ДЛ-1/05 вн);
* Устав АНО «ФИРОН».

Программа направлена на качественное изменение профессиональных компетенций, необходимых для выполнения вида профессиональной деятельности

«ВПД 1. Проектирование, разработка и оптимизация веб-приложений» в рамках имеющейся квалификации

ПК 1.1 Осуществлять аудит безопасности веб-приложения в соответствии с регламентами по безопасности;

ПК 1.2 Производить тестирование разработанного веб приложения;

ПК 1.3 Управлять доступом к данным и определять уровни прав пользователей ИР;

ПК 1.4 Обеспечивать безопасную и бесперебойную работу сайта;

ПК 1.5 Организовывать работы по обеспечению безопасной работы ИР.

По окончании обучения выдается удостоверение о повышении квалификации.

|  |
| --- |
|  |
| **Автономная некоммерческая организация инновационного развития образования и науки «ФИРОН» (АНО «ФИРОН»)** |

|  |  |
| --- | --- |
|  | **УТВЕРЖДАЮ**  Директор АНО «ФИРОН»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.С. Шенгоф  «23» октября 2020 г. |

**ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА**

|  |
| --- |
| «Основы безопасной веб-разработки» |

(наименование программы)

|  |  |
| --- | --- |
| **Вид программы:** | повышение квалификации |

|  |  |
| --- | --- |
| **Объем в часах:** | 72 |

|  |  |
| --- | --- |
| **Организация обучения:** | 2 недели  с использованием дистанционных образовательных технологий |

г. Ростов-на-Дону, 2020

**ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ**

**1. Цель программы**

формирование у слушателей профессиональных компетенций, необходимых при разработке и поддержке безопасных web-приложений для успешного выполнения профессиональных задач.

Основные задачи программы:

– систематизировать знания слушателей о видах уязвимостей;

– сформировать представления слушателей о методах и средствах защиты веб-приложений от потенциальных угроз.

**2. Планируемые результаты обучения:**

2.1. Знание (осведомленность в областях)

- основы информационной безопасности web-ресурсов;

- сетевые протоколы и основы web-технологий;

- основные уязвимости и атаки на web-приложения;

- методы поиска уязвимостей web-приложений;

- источники угроз информационной безопасности и меры по их предотвращению;

- современные программно-технические средства и способы обеспечения безопасности ИР;

- методы и средства защиты web-приложений;

- принципы разработки безопасных систем аутентификации;

- принципы организации безопасности внутри корпоративной сети.

2.2. Умение (способность к деятельности)

- находить и определять уязвимости в web-приложениях;

- применять принципы эксплуатации уязвимостей в коде;

- проводить аудит сетевой безопасности ;

- назначать права доступа пользователей к модулям, данным и разделам ИР;

- изменять права доступа пользователей к модулям, данным и разделам ИР;

- применять специальные процедуры по управлению правами доступа пользователей ИР;

- контролировать соблюдение прав доступа пользователей ИР;

- мониторить атаки на ИР и выполнять соответствующие действия;

- производить настройку параметров web-сервера;

- идентифицировать инциденты нарушения безопасной работы и принимать решение по изменению регламентных процедур

- выполнять работы по организации функционирования систем защиты информации;

- составлять модель угроз информационной безопасности;

- осуществлять оптимизацию web-приложения с целью повышения уровня его безопасности;

- разрабатывать программный код клиентской и серверной части web-приложений с учетом требований к уровню безопасности.

2.3. Навыки (использование конкретных инструментов)

- использовании средств аудита безопасности;

- выявлении уязвимостей с использованием различных средств анализа защищенности;

- настройке систем безопасности web-приложений;

- выполнении разработки и проектирования информационных систем с учетом требований к уровню безопасности;

- модернизации веб-приложений с учетом требований к уровню безопасности.

**3. Категория слушателей** (возможно заполнение не всех полей)

* 1. Среднее профессиональное и (или) высшее образование
  2. Не требуется
  3. Не требуется
  4. Не требуется

**4. Учебный план программы «Основы безопасной веб-разработки»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Модуль | Всего, час | Виды учебных занятий | | |
| лекции | практические занятия | самостоятельная работа |
| 1 | Модуль 1. Криптографическая защита информации | 19 | 5 | 7 | 7 |
| 2 | Модуль 2. Веб безопасность | 17 | 3 | 7 | 7 |
| 3 | Модуль 3. Разграничение прав доступа | 9 | 2 | 3 | 4 |
| 4 | Модуль 4. Безопасность компьютерных сетей | 13 | 3 | 3 | 7 |
| 5 | Модуль 5. Анонимность в сети | 8 | 2 | 2 | 4 |
|  | Итоговая аттестация | 6 |  | 6 |  |
|  | Всего | **72** | **15** | **28** | **29** |
| Итоговая аттестация | |  | Указывается вид (экзамен, зачёт, реферат и т.д.) | | |
| тестирование | | 6 |  | | |

**5. Календарный план-график реализации образовательной** программы

(дата начала обучения – дата завершения обучения) в текущем календарном году, указания на периодичность набора групп (не менее 1 группы в месяц)

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование учебных модулей | Трудоёмкость (час) | Сроки обучения |
| 1 | Модуль 1. Криптографическая защита информации | 19 | 1-5 ноября |
| 2 | Модуль 2. Веб безопасность | 17 | 6-8 ноября |
| 3 | Модуль 3. Разграничение прав доступа | 9 | 9-10 ноября |
| 4 | Модуль 4. Безопасность компьютерных сетей | 13 | 11-13 ноября |
| 5 | Модуль 5. Анонимность в сети | 8 | 14 ноября |
| 6 | Итоговая аттестация | 6 | 15 ноября |
| Всего: | | 72 | 1-15 ноября |

**6. Учебно-тематический план программы «Основы безопасной веб-разработки»**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Модуль / Тема | Всего, час | Виды учебных занятий | | | | Формы контроля | |
| лекции | практические занятия | самостоятельная работа |  | |
| **1.** | **Модуль 1. Криптографическая защита информации** | **19** | **5** | **7** | **7** | **тест** | |
| 1.1 | HTTPS | 6 | 2 | 2 | 2 |  | |
| 1.2. | Криптография для веб-разработчиков | 6 | 2 | 2 | 2 |  | |
| 1.3. | Аутентификация | 7 | 1 | 3 | 3 |  | |
| **2.** | **Модуль 2. Веб безопасность** | **17** | **3** | **7** | **7** | **тест** | |
| 2.1 | Web security (OWASP) | 3 | 1 |  | 2 |  | |
| 2.2 | Тестирование безопасности веб приложений | 5 | 1 | 2 | 2 |  | |
| 2.3 | Инъекции | 9 | 1 | 5 | 3 |  | |
| **3.** | **Модуль 3. Разграничение прав доступа** | **9** | **2** | **3** | **4** | **тест** | |
| 3.1. | Привилегии Linux | 3 | 1 |  | 2 |  | |
| 3.2 | Привилегии Windows | 6 | 1 | 3 | 2 |  | |
| **4.** | **Модуль 4. Безопасность компьютерных сетей** | **13** | **3** | **3** | **7** | **тест** | |
| 4.1 | Безопасность сетей | 3 | 1 |  | 2 |  | |
| 4.2 | Безопасность сетей на практике | 3 | 1 |  | 2 |  | |
| 4.3 | Безопасность в облаке | 7 | 1 | 3 | 3 |  | |
| **5.** | **Модуль 5. Анонимность в сети** | **8** | **2** | **2** | **4** | **тест** | |
| 5.1 | Анонимность в сети | 3 | 1 |  | 2 |  | |
| 5.2 | Browser fingerprint | 5 | 1 | 2 | 2 |  | |
|  | Итоговая аттестация | 6 |  | 6 |  | тест | |
|  | Всего | **72** | **15** | **28** | **29** |  | |

**7. Учебная (рабочая) программа повышения квалификации   
«Основы безопасной веб-разработки»**

**Модуль 1. Криптографическая защита информации (19 ак.ч)**

Тема 1. HTTPS. MITM, ARP-SPOOFING, HTTPS, Шифрование, TLS, Цифровые сертификаты, DNS over HTTPS

Тема 2. Криптография для веб-разработчиков. Аутентификация, Шифрование, Хэш-функции, Цифровая подпись, Криптографические протоколы

Тема 3. Аутентификация. Аутентификация, Пароль, Проблема утечки паролей, Брутфорс, Уязвимость паролей, Схемы аутентификации, Биометрия, Многофакторная аутентификация.

**Модуль 2. Веб безопасность (17 ак.ч.)**

Тема 1. Web security (OWASP). OWASP, Инъекции, Аутентификация, Авторизация, Хэширование, Радужные таблицы, Соль для паролей, XSS, Deserialization, Логирование

Тема 2. Тестирование безопасности веб приложений. XSS сохраненный и отраженный, Предотвращение XSS, SQL-injection, No-SQL-injection, Предотвращение инъекций, XXE, CSRF, Path traversal, Burp Suite, Брутфорсинг, Статический анализ кода, Фаззинг

Тема 3. Инъекции. Защита от инъекций, Слепые инъекции, Sql Map, CSS инъекции, Защита от XSS, Пэйлоад, Инъекции в bash, Уязвимости DNS имен, Кейлоггер

**Модуль 3. Разграничение прав доступа (9 ак.ч.)**

Тема 1. Привилегии Linux. Уровни доступа, Пользователи, Группы, Права доступа, Владелец файла, Права доступа к процессу, Права доступа к сети, Права суперпользователя

Тема 2. Привилегии Windows. Типы учетных записей, Active Directory, Пользователи, Группы, Права доступа, Владелец файла, Права доступа к процессу, Права доступа к сети, UAC, SID, DACL, Типы доступа

**Модуль 4. Безопасность компьютерных сетей (13 ак.ч.)**

Тема 1. Безопасность сетей. TCP/IP стек, TCP, UDP, IP, MAC addr, ICMP, BGP, DNS, DHCP, SYN flooding, ARP спуфинг, DoS, Hijacking connection

Тема 2. Безопасность сетей на практике. Роль сетевой безопасности, Виды сетевого сканирования, ARP-сканирование, Определение вида оборудования, Nmap, Shodan, Firewall, Iptables, Netfilter, IDS/IPS, Honeypot, NAT

Тема 3. Безопасность в облаке. DDos, Облачная инфраструктура, VLAN, API, CloudFlare, Firewall, WAF, Системы мониторинга, Логирование, ACL, SSO, Бэкап, CI/CD, Chaos monkey, Социальная инженерия

**Модуль 5. Анонимность в сети (8 ак.ч)**

Тема 1. Анонимность в сети. Понятие анонимности, Необходимость анонимизации, Модель угроз, Цифровой отпечаток, VPN

Тема 2. Browser fingerprint. Цифровой профиль, Пассивный цифровой отпечаток, Активный цифровой отпечаток, Анонимность, Трекеры пользователей, Заголовки HTTP, Энтропия параметров, Хранилище браузера, OpenDatabase, HPKP, TorBrowser, Do Not Track

**Описание практико-ориентированных заданий и кейсов**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Номер темы/модуля | Наименование практического занятия | Описание |
| 1.1 | 1 | HTTPS | MITM, ARP-SPOOFING, HTTPS, Шифрование, TLS, Цифровые сертификаты, DNS over HTTPS |
| 1.2 | 1 | Криптография для веб-разработчиков | Аутентификация, Шифрование, Хэш-функции, Цифровая подпись, Криптографические протоколы |
| 1.3. | 1 | Аутентификация | Аутентификация, Пароль, Проблема утечки паролей, Брутфорс, Уязвимость паролей, Схемы аутентификации, Биометрия, Многофакторная аутентификация |
| 2.1 | 2 | Web security (OWASP) | OWASP, Инъекции, Аутентификация, Авторизация, Хэширование, Радужные таблицы, Соль для паролей, XSS, Deserialization, Логирование |
| 2.2 | 2 | Тестирование безопасности веб приложений | XSS сохраненный и отраженный, Предотвращение XSS, SQL-injection, No-SQL-injection, Предотвращение инъекций, XXE, CSRF, Path traversal, Burp Suite, Брутфорсинг, Статический анализ кода, Фаззинг |
| 2.3 | 2 | Инъекции | Защита от инъекций, Слепые инъекции, Sql Map, CSS инъекции, Защита от XSS, Пэйлоад, Инъекции в bash, Уязвимости DNS имен, Кейлоггер |
| 3.1 | 3 | Привилегии Linux | Уровни доступа, Пользователи, Группы, Права доступа, Владелец файла, Права доступа к процессу, Права доступа к сети, Права суперпользователя |
| 3.2 | 3 | Привилегии Windows | Типы учетных записей, Active Directory, Пользователи, Группы, Права доступа, Владелец файла, Права доступа к процессу, Права доступа к сети, UAC, SID, DACL, Типы доступа |
| 4.1 | 4 | Безопасность сетей | TCP/IP стек, TCP, UDP, IP, MAC addr, ICMP, BGP, DNS, DHCP, SYN flooding, ARP спуфинг, DoS, Hijacking connection |
| 4.2 | 4 | Безопасность сетей на практике | Роль сетевой безопасности, Виды сетевого сканирования, ARP-сканирование, Определение вида оборудования, Nmap, Shodan, Firewall, Iptables, Netfilter, IDS/IPS, Honeypot, NAT |
| 4.3 | 4 | Безопасность в облаке | DDos, Облачная инфраструктура, VLAN, API, CloudFlare, Firewall, WAF, Системы мониторинга, Логирование, ACL, SSO, Бэкап, CI/CD, Chaos monkey, Социальная инженерия |
| 5.1 | 5 | Анонимность в сети | Понятие анонимности, Необходимость анонимизации, Модель угроз, Цифровой отпечаток, VPN |
| 5.2 | 5 | Browser fingerprint | Цифровой профиль, Пассивный цифровой отпечаток, Активный цифровой отпечаток, Анонимность, Трекеры пользователей, Заголовки HTTP, Энтропия параметров, Хранилище браузера, OpenDatabase, HPKP, TorBrowser, Do Not Track |

**8. Оценочные материалы по образовательной программе**

**8.1. Вопросы тестирования по модулям**

|  |  |  |  |
| --- | --- | --- | --- |
| № модуля | Вопросы входного тестирования | Вопросы промежуточного тестирования | Вопросы итогового тестирования |
| 1.1 | Оцените свои знания в сфере безопасной веб-разработки | Модуль 1.  1. Если данные необходимо зашифровать и сжать, в каком порядке это лучше делать?  a. не имеет значения  b. зависит от данных и алгоритмов  c. сначала сжатие, потом шифрование  d. сначала шифрование, потом сжатие  2. В случае, если на сервере хранится хеш от пароля, что следует пересылать во время аутентификации?  a. не имеет значения  b. хеш  c. пароль  3. В случае, если для некоторого значения мы можем эффективно найти другое значение, дающее такой же хеш, это значит, что хеш-функция  a. нестойка к восстановлению первого прообраза  b. нестойка к восстановлению первого прообраза  c. нестойка к коллизиям  4. Протокол Диффи-Хеллмана устойчив к  a. прослушке канала  b. mitm с подменой сообщений  c. ‘r’ на ‘/foo/’  d. их owner  5. Для большей эффективности по производительности используется:  a. сессионный симметричный ключ, зашифрованный ассиметричным  b. сессионный асимметричный ключ, зашифрованный симметричным  6. Для создания ЭЦП используется  a. закрытый ассиметричный ключ  b. симметричный ключ  c. открытый асимметричный ключ  7. Что устойчивее к ограниченному перебору?  a. пароль  b. биометрическая система  8. Что обеспечивает TLS? (выберите несколько)  a. Аутентификацию сервера  b. Аутентификацию клиента  c. Шифрование передаваемых данных  d. Защиту от XSS  9. HSTS обеспечивает: (выберите несколько)  a. Невозможность соединения при ошибках TLS  b. Защиту от CSRF  c. Защиту от DoS-атак  d. Невозможность перейти на HTTP-версию страницы  10. Авторизация это… (выберите один)  a. процесс проверки подлинности чего-либо  b. предоставление определённому лицу или группе лиц прав на выполнение определенных действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий  c. процедура, в результате выполнения которой для субъекта выявляется его уникальный дескриптор | 1 этап. XSS: обход аутентификации, похищение cookie залогиненного пользователя.  2 этап. SQL injection: извлечение хеша администратора из БД, получение пароля администратора через хеш.  3 этап. Десериализация c получением доступа к shell сервера. |
| 1.2 |  | Модуль 2.  1. При настройке файрвола, какой принцип является корректным?  a. Запретить по умолчанию  b. Разрешить по умолчанию  2. DDoS атака это ...  a. получение доступа к приватным данным на сервере  b. получение доступа к приватным данным на клиенте  c. атака цель которой спровоцировать отказ сервиса  d. распределенная атака цель которой спровоцировать отказ сервиса  3. В какие из следующих языков возможно проведение инъекции? (выберите несколько)  a. sql  b. javascript  c. html  d. bash  4. Эффективным способом защиты от SQL-инъекций является: (выберите несколько)  a. экранирование входных параметров  b. использование параметризованных запросов  c. фильтрация данных на предмет наличия ключевых слов или спецсимволов  d. использование нестандартных имен таблиц и полей  5. Что такое Соль с точки зрения веб-безопасности?  a. используется для защиты запросов при передаче в интернет  b. примешивается к паролю, злоумышленник не знает его  c. примешивается к паролю перед хешированием, уникальна для каждого пароля  d. применяется в криптографических алгоритмах авторизации  6. Уязвимы ли No-SQL базы данных для инъекций?  a. да  b. нет  c. уязвимы, но только старые версии  7. Для чего используется CSRF токен?  a. для авторизации пользователя  b. для аутентификации пользователя  c. в качестве сессионного ключа  d. для защиты от межсайтовой подделки запроса  8. В чем суть XSS атаки?  a. удаленном выполнении кода на стороне сервера  b. выполнение JS кода, размещенного другим пользователем, на стороне клиента  c. выполнение SQL скрипта, размещенного другим пользователем, на стороне клиента  d. похищение приватных данных пользователя  9. Радужные таблицы используются для:  a. облегчения процесса поиска пароля по его хэшу  b. увеличению скорости вычисление хэша  c. оптимизации потребления памяти при работе хэш-функции  10. В чем суть фаззинга?  a. передача приложению заранее подготовленных данных  b. передача приложению данных сгенерированных нейронной сетью  c. передача приложению случайных данных на ввод |  |
| 1.3. |  | Модуль 3.  1. При выполнении команды touch /foo/x/d проверяются  a. ‘r’ на ‘/foo/x/d’  b. ‘x’ на ‘/’  c. ‘r’ на ‘/foo/’  d. ‘w’ на ‘/foo/x/’  2. suid binaries запускаются от  a. текущего пользователя  b. суперпользователя  c. ‘r’ на ‘/foo/’  d. их owner  3. Когда проверяются права на файл в Linux-системах?  a. при открытии файла  b. при каждом обращении  4. Для чего используется файл /etc/shadow?  a. хранение логинов пользователей  b. хранение паролей пользователей  c. хранение хэшей паролей пользователей  d. хранения групп пользователей  5. Команда chmod u+rw test.txt сделает следующее:  a. дает пользователю права на чтение файла  b. дает пользователю права на выполнение и запись файла  c. дает пользователю права на чтение и запись файла  d. дает всем пользователям права на чтение и запись файла  6. UAC это…  a. система контроля учетных записей пользователей в Windows  b. система контроля прав выполнения программ  c. система контроля учетных записей пользователей Linux  d. система мандатного управления доступом  7. Active Directory позволяет: (выберите несколько)  a. использовать групповые политики  b. устанавливать программное обеспечение на доменные компьютеры  c. изменять дисковые квоты пользователям  d. выдавать IP адреса узлам сети  8. Как повысить привилегии в Linux:  a. sudo su  b. sudo команда  c. upuser  d. useradd permission |  |
| 1.4. |  | Модуль 4.  1. nmap позволяет (выберите несколько):  a. сканировать порты  b. определять программное обеспечение  c. определять версию ПО  d. эксплуатировать уязвимости ПО  2. ARP-сканирование позволяет (выберите несколько):  a. сканировать узлы сети почти не оставляя следов  b. сканировать открытые порты  c. сканировать узлы сети в пассивном режиме  d. сканировать версии прошивок сетевого оборудования  3. MAC адрес всегда содержит в себе информацию:  a. о производителе оборудования  b. о версии прошивки оборудования  c. о модели оборудования  d. о IP адресе устройства  4. iptables это...  a. файрвол  b. утилита управления файрволом  c. утилита формирования таблиц маршрутизации  d. таблица со списком IP адресов узлов сети  5. VLAN позволяет...  a. изолировать компьютеры в виртуальной сети  b. администрировать права доступа к сетевым службам  c. увеличивать пропускную способность сетевых устройств  6. WAF использует для защиты приложения (множественный выбор):  a. сигнатурный анализ  b. черные списки IP адресов  c. поведенческий анализ  d. сверяет каждый запрос с белым списком  7. ACL это...  a. список данных о пользователях  b. список управления доступом  c. список разрешенных правил файрвола  8. IP протокол в модели TCP/IP обеспечивает:  a. маршрутизацию пакетов между различными сегментами сети  b. гарантированную доставку пакета  c. доставку пакетов в правильной последовательности  d. получение IP адреса по имени хоста  9. TCP протокол в модели TCP/IP обеспечивает:  a. целостность потока пакетов, передаваемых по сети  b. нахождение получателя пакета в сети  c. шифрование данных передаваемых по сети  10. UDP протокол обладает следующими особенностями (выберите несколько):  a. обеспечивает надежную передачу данных через сеть  b. позволяет добиться большей скорости передачи данных  c. гарантирует отсутствие дубликатов пакетов  d. udp пакет содержит в себе порт получателя и порт отправителя пакета |  |
| 1.5 |  | Модуль 5.  1. Анонимность - это вообще законно?  a. Нет, ею пользуются только преступники.  b. Да, каждый человек имеет права скрывать о себе любую информацию в любое время.  c. Зависит от конкретной ситуации.  2. С точки зрения угроз информации деанонимизация это  a. Угроза доступности  b. Угроза конфиденциальности  c. Угроза целостности  3. Вы заселились в гостиницу под чужим именем. Чего вы добились?  a. Уголовного наказания.  b. Анонимности.  c. Псевдонимности.  4. Кому нужно вас деанонимизировать?  a. Преступникам  b. Государству  c. Зависит от модели угроз  d. Рекламщикам  5. На какой вопрос нет необходимости отвечать, когда вы составляете модель угроз.  a. Кто потенциальный злоумышленник?  b. Что вы защищаете?  c. Зачем вы это защищаете?  d. От чего вы защищаете?  6. Сайты знают о нас многое. А что они не знают?  a. Разрешение экрана  b. Установленные в системе шрифты  c. Версию BIOS  d. Плагины браузера  7. Крупные IT-корпорации потенциально могут знать о нас всё. Могут, но, что их ограничивает в этом? Возможно несколько вариантов ответа  a. Знать всё это дорого.  b. У них нет права на сбор любой информации.  c. Информация может быть технически недоступна.  8. Кто "покупатель" информации о вас?  a. Иллюминаты.  b. Продавцы рекламных услуг.  c. Сплетницы сидящие у моего подъезда.  d. Никто. Моя информация никому не нужна.  9. Какие средства анонимизации существуют? Можно выбрать несколько вариантов  a. Анонимные средств оплаты  b. Анонимные средства просмотра сайтов  c. Анонимные почты  d. Анонимные прокси-сервера  10. Можно ли быть анонимным (псевдонимным) полностью?  a. Да  b. Нет |  |

**8.2.** Для оценивания результатов освоения программы используется рейтинговая шкала баллов, формирующихся по результатам успешного выполнения слушателем элементов программы. Максимальная сумма баллов рейтинга по программе - 100.

Промежуточная аттестация и контроль качества усвоения знаний

Проверка качества усвоения лекционных, учебно-методических материалов и самостоятельно изучаемых слушателями источников литературы проводится в различной форме:

- текущий контроль выполнения лабораторных работ проводится в форме экспертного наблюдения, в ходе которого слушателю может быть начислено до 18 баллов;

- промежуточная аттестация проводится в форме тестирований, за успешное выполнение которых слушателю может быть начислено до 52 баллов;

Итоговая аттестация качества усвоения знаний

Итоговая аттестация проводится в виде экзаменационной работы, представляющей собой комплексное задание по всем разделам образовательной программы, за успешное выполнение которого может быть начислено до 30 баллов.

**8.3.** В рамках итоговой аттестации слушатели курса выполняют тестовое задание.

**Тестовые задания для подготовки к промежуточной аттестации**

**Модуль 1.**

1. Если данные необходимо зашифровать и сжать, в каком порядке это лучше делать?
   1. не имеет значения
   2. зависит от данных и алгоритмов
   3. сначала сжатие, потом шифрование
   4. сначала шифрование, потом сжатие
2. В случае, если на сервере хранится хеш от пароля, что следует пересылать во время аутентификации?
   1. не имеет значения
   2. хеш
   3. пароль
3. В случае, если для некоторого значения мы можем эффективно найти другое значение, дающее такой же хеш, это значит, что хеш-функция
   1. нестойка к восстановлению первого прообраза
   2. нестойка к восстановлению первого прообраза
   3. нестойка к коллизиям
4. Протокол Диффи-Хеллмана устойчив к
   1. прослушке канала
   2. mitm с подменой сообщений
   3. ‘r’ на ‘/foo/’
   4. их owner
5. Для большей эффективности по производительности используется:
   1. сессионный симметричный ключ, зашифрованный ассиметричным
   2. сессионный асимметричный ключ, зашифрованный симметричным
6. Для создания ЭЦП используется
   1. закрытый ассиметричный ключ
   2. симметричный ключ
   3. открытый асимметричный ключ
7. Что устойчивее к ограниченному перебору?
   1. пароль
   2. биометрическая система
8. Что обеспечивает TLS? (выберите несколько)
   1. Аутентификацию сервера
   2. Аутентификацию клиента
   3. Шифрование передаваемых данных
   4. Защиту от XSS
9. HSTS обеспечивает: (выберите несколько)
   1. Невозможность соединения при ошибках TLS
   2. Защиту от CSRF
   3. Защиту от DoS-атак
   4. Невозможность перейти на HTTP-версию страницы
10. Авторизация это… (выберите один)
    1. процесс проверки подлинности чего-либо
    2. предоставление определённому лицу или группе лиц прав на выполнение определенных действий; а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий
    3. процедура, в результате выполнения которой для субъекта выявляется его уникальный дескриптор

**Модуль 2.**

1. При настройке файрвола, какой принцип является корректным?
   1. Запретить по умолчанию
   2. Разрешить по умолчанию
2. DDoS атака это ...
   1. получение доступа к приватным данным на сервере
   2. получение доступа к приватным данным на клиенте
   3. атака цель которой спровоцировать отказ сервиса
   4. распределенная атака цель которой спровоцировать отказ сервиса
3. В какие из следующих языков возможно проведение инъекции? (выберите несколько)
   1. sql
   2. javascript
   3. html
   4. bash
4. Эффективным способом защиты от SQL-инъекций является: (выберите несколько)
   1. экранирование входных параметров
   2. использование параметризованных запросов
   3. фильтрация данных на предмет наличия ключевых слов или спецсимволов
   4. использование нестандартных имен таблиц и полей
5. Что такое Соль с точки зрения веб-безопасности?
   1. используется для защиты запросов при передаче в интернет
   2. примешивается к паролю, злоумышленник не знает его
   3. примешивается к паролю перед хешированием, уникальна для каждого пароля
   4. применяется в криптографических алгоритмах авторизации
6. Уязвимы ли No-SQL базы данных для инъекций?
   1. да
   2. нет
   3. уязвимы, но только старые версии
7. Для чего используется CSRF токен?
   1. для авторизации пользователя
   2. для аутентификации пользователя
   3. в качестве сессионного ключа
   4. для защиты от межсайтовой подделки запроса
8. В чем суть XSS атаки?
   1. удаленном выполнении кода на стороне сервера
   2. выполнение JS кода, размещенного другим пользователем, на стороне клиента
   3. выполнение SQL скрипта, размещенного другим пользователем, на стороне клиента
   4. похищение приватных данных пользователя
9. Радужные таблицы используются для:
   1. облегчения процесса поиска пароля по его хэшу
   2. увеличению скорости вычисление хэша
   3. оптимизации потребления памяти при работе хэш-функции
10. В чем суть фаззинга?
    1. передача приложению заранее подготовленных данных
    2. передача приложению данных сгенерированных нейронной сетью
    3. передача приложению случайных данных на ввод

**Модуль 3.**

1. При выполнении команды touch /foo/x/d проверяются
   1. ‘r’ на ‘/foo/x/d’
   2. ‘x’ на ‘/’
   3. ‘r’ на ‘/foo/’
   4. ‘w’ на ‘/foo/x/’
2. suid binaries запускаются от
   1. текущего пользователя
   2. суперпользователя
   3. ‘r’ на ‘/foo/’
   4. их owner
3. Когда проверяются права на файл в Linux-системах?
   1. при открытии файла
   2. при каждом обращении
4. Для чего используется файл /etc/shadow?
   1. хранение логинов пользователей
   2. хранение паролей пользователей
   3. хранение хэшей паролей пользователей
   4. хранения групп пользователей
5. Команда *chmod u+rw test.txt* сделает следующее:
   1. дает пользователю права на чтение файла
   2. дает пользователю права на выполнение и запись файла
   3. дает пользователю права на чтение и запись файла
   4. дает всем пользователям права на чтение и запись файла
6. UAC это…
   1. система контроля учетных записей пользователей в Windows
   2. система контроля прав выполнения программ
   3. система контроля учетных записей пользователей Linux
   4. система мандатного управления доступом
7. Active Directory позволяет: (выберите несколько)
   1. использовать групповые политики
   2. устанавливать программное обеспечение на доменные компьютеры
   3. изменять дисковые квоты пользователям
   4. выдавать IP адреса узлам сети
8. Как повысить привилегии в Linux:
   1. sudo su
   2. sudo *команда*
   3. upuser
   4. useradd permission

**Модуль 4.**

1. nmap позволяет (выберите несколько):
   1. сканировать порты
   2. определять программное обеспечение
   3. определять версию ПО
   4. эксплуатировать уязвимости ПО
2. ARP-сканирование позволяет (выберите несколько):
   1. сканировать узлы сети почти не оставляя следов
   2. сканировать открытые порты
   3. сканировать узлы сети в пассивном режиме
   4. сканировать версии прошивок сетевого оборудования
3. MAC адрес всегда содержит в себе информацию:
   1. о производителе оборудования
   2. о версии прошивки оборудования
   3. о модели оборудования
   4. о IP адресе устройства
4. iptables это...
   1. файрвол
   2. утилита управления файрволом
   3. утилита формирования таблиц маршрутизации
   4. таблица со списком IP адресов узлов сети
5. VLAN позволяет...
   1. изолировать компьютеры в виртуальной сети
   2. администрировать права доступа к сетевым службам
   3. увеличивать пропускную способность сетевых устройств
6. WAF использует для защиты приложения (множественный выбор):
   1. сигнатурный анализ
   2. черные списки IP адресов
   3. поведенческий анализ
   4. сверяет каждый запрос с белым списком
7. ACL это...
   1. список данных о пользователях
   2. список управления доступом
   3. список разрешенных правил файрвола
8. IP протокол в модели TCP/IP обеспечивает:
   1. маршрутизацию пакетов между различными сегментами сети
   2. гарантированную доставку пакета
   3. доставку пакетов в правильной последовательности
   4. получение IP адреса по имени хоста
9. TCP протокол в модели TCP/IP обеспечивает:
   1. целостность потока пакетов, передаваемых по сети
   2. нахождение получателя пакета в сети
   3. шифрование данных передаваемых по сети
10. UDP протокол обладает следующими особенностями (выберите несколько):
    1. обеспечивает надежную передачу данных через сеть
    2. позволяет добиться большей скорости передачи данных
    3. гарантирует отсутствие дубликатов пакетов
    4. udp пакет содержит в себе порт получателя и порт отправителя пакета

**Модуль 5.**

1. Анонимность - это вообще законно?
   1. Нет, ею пользуются только преступники.
   2. Да, каждый человек имеет права скрывать о себе любую информацию в любое время.
   3. Зависит от конкретной ситуации.
2. С точки зрения угроз информации деанонимизация это
   1. Угроза доступности
   2. Угроза конфиденциальности
   3. Угроза целостности
3. Вы заселились в гостиницу под чужим именем. Чего вы добились?
   1. Уголовного наказания.
   2. Анонимности.
   3. Псевдонимности.
4. Кому нужно вас деанонимизировать?
   1. Преступникам
   2. Государству
   3. Зависит от модели угроз
   4. Рекламщикам
5. На какой вопрос нет необходимости отвечать, когда вы составляете модель угроз.
   1. Кто потенциальный злоумышленник?
   2. Что вы защищаете?
   3. Зачем вы это защищаете?
   4. От чего вы защищаете?
6. Сайты знают о нас многое. А что они не знают?
   1. Разрешение экрана
   2. Установленные в системе шрифты
   3. Версию BIOS
   4. Плагины браузера
7. Крупные IT-корпорации потенциально могут знать о нас всё. Могут, но, что их ограничивает в этом? Возможно несколько вариантов ответа
   1. Знать всё это дорого.
   2. У них нет права на сбор любой информации.
   3. Информация может быть технически недоступна.
8. Кто "покупатель" информации о вас?
   1. Иллюминаты.
   2. Продавцы рекламных услуг.
   3. Сплетницы, сидящие у моего подъезда.
   4. Никто. Моя информация никому не нужна.
9. Какие средства анонимизации существуют? Можно выбрать несколько вариантов
   1. Анонимные средств оплаты
   2. Анонимные средства просмотра сайтов
   3. Анонимные почты
   4. Анонимные прокси-сервера
10. Можно ли быть анонимным (псевдонимным) полностью?
    1. Да
    2. Нет

**8.4.** Экзаменационная работа представляет собой задание на исследование сайта на уязвимости. Слушатель получает виртуальную машину с Kali Linux в качестве инструмента. Необходимо провести исследование безопасности сайта, обнаружить уязвимости и поэксплуатировать их, получив содержимое каталога файловой системы сервера.

1 этап. XSS: обход аутентификации, похищение cookie залогиненного пользователя.

2 этап. SQL injection: извлечение хеша администратора из БД, получение пароля администратора через хеш.

3 этап. Десериализация c получением доступа к shell сервера.

**8.5.** Измерительное испытание в начале обучения проводится в форме опроса об уровне знаний в сфере безопасной веб-разработки, итоговая аттестация проводится в итогового практического задания. Промежуточная аттестация по модулям осуществляется в результате оценки выполнения практико-ориентированных заданий.

При подготовке к выполнению тестовых заданий обучающиеся используют весь учебный материал курса, источники основной и дополнительной литературы, ресурсы Интернет. Тестовые задания рассчитаны на самостоятельную работу без использования вспомогательных материалов. Для выполнения следует внимательно прочитать поставленный вопрос. После ознакомления с вопросом следует приступать к прочтению предлагаемых вариантов ответа. Необходимо прочитать все варианты и в качестве ответа следует выбрать один или несколько соответствующих правильному ответу. На выполнение тестов отводится не более 2 академических часов.

Методические указания. При подготовке к выполнению тестовых заданий обучающиеся используют весь учебный материал курса, источники основной и дополнительной литературы, ресурсы Интернет. Тестовые задания рассчитаны на самостоятельную работу без использования вспомогательных материалов. Для выполнения следует внимательно прочитать поставленный вопрос. После ознакомления с вопросом следует приступать к прочтению предлагаемых вариантов ответа. Необходимо прочитать все варианты и в качестве ответа следует выбрать один или несколько соответствующих правильному ответу. На выполнение экзамена отводится ограниченное время.

**9.Организационно-педагогические условия реализации программы**

**9.1. Кадровое обеспечение программы**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| №  п/п | Фамилия, имя, отчество (при наличии) | Место основной работы и должность, ученая степень и ученое звание (при наличии) | Ссылки на веб-страницы с портфолио (при наличии) | Фото в формате jpeg | Отметка о полученном согласии на обработку персональных данных |
| 1. | Гуфан Константин Юрьевич | Кандидат математических наук, Зам.директора по научной работе ФГАНУ НИИ «Спецвузавтоматика» |  |  | + |
| 2 | Маликов Тимур Абдулаевич | Реверс-инженер ФГАНУ НИИ «Спецвузавтоматика» |  |  | + |
| 3 | Шаповалов Василий Николаевич | Технический директор Р2Р |  |  | + |
| 4 | Уралов Александр Васильевич | Зав.лабораторией ФГАНУ НИИ «Спецвузавтоматика» |  |  | + |
| 5 | Васильев Андрей Владимирович | Программист ФГАНУ НИИ «Спецвузавтоматика» |  |  | + |
| 6 | Уланов Константин Владимирович | Программист ФГАНУ НИИ «Спецвузавтоматика» |  |  | + |
| 7 | Иванов Сергей Сергеевич | Frontend-разработчик |  |  | + |
|  | Тюрин  Кай Андреевич | Заведующий центром ФГАНУ НИИ «Спецвузавтоматика |  |  |  |

**9.2. Учебно-методическое обеспечение и информационное сопровождение**

|  |  |
| --- | --- |
| Учебно-методические материалы | |
| Методы, формы и технологии | Методические разработки,  материалы курса, учебная литература |
| Технология электронного интерактивного обучения с использованием LMS Moodle  Технология онлайн-обучения  Вебинары  Индивидуальная форма работы  Методы самостоятельной работы: методы работы с конспектами, решение практических заданий, проблемно-эвристический метод | 1. Андерсон, Р. Инженерия безопасности [Ross Anderson. Security Engineering]. — N.Y.: John Wiley & Sons, 2020. - 612 с.  2. Фергюсон Н., Шнайер Б. Практическая криптография / Н. Фергюсон, Б. Шнайер. – М.: Вильямс, 2017. – 420 с.  3. Эриксон, Дж. Хакинг. Искусство эксплойта / Дж. Эриксон. - – Санкт-Петербург: Питер, 2018. – 496 с.  4. David A. Wheeler Secure Programming HOWTO: сайт. – URL:  https://dwheeler.com/secure-programs/Secure-Programs-HOWTO.pdf (дата обращения: 30.08.2020). – Текст: электронный.  5. Кицца, Дж.М. Руководство по безопасности компьютерной сети [Kizza, J.M. Guide to Computer Network Security]/Дж.М.Кицца. - University of Tennessee: Springer International Publishing AG, 2017. – 596 с.  6. Сивер, Э. Линукс в двух словах, 6-е издание [Siever, E., Figgins, S., Love, R., Robbins, A. Linux in a Nutshell, 6th Edition]. –Sebastopol, O'Reilly Media, Inc., 2018. – 944 с.  7. Зайтц, Дж. Программирование на Python для хакеров [Justin Seitz Black Hat Python].- San Francisco: No Starch Press, 2014. - 192 с. |

|  |  |
| --- | --- |
| Информационное сопровождение | |
| Электронные  образовательные ресурсы | Электронные  информационные ресурсы |
| Курс Computer Systems Security, Massachusetts Institute of Technology. – сайт. URL:  https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-858-computer-systems-security-fall-2014/ (дата обращения: 30.05.2020). | DNSSEC – что это такое и почему эта технология так важна? - Текст: электронный // Icann.com: Интернет-портал. – URL: https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-20-ru (дата обращения: 30.08.2020). |
| Визуализация принципов работы TLS – Текст: электронный // Catchpoint.com: Интернет-портал. – URL: https://blog.catchpoint.com/2017/05/12/dissecting-tls-using-wireshark/ (дата обращения: 30.08.2020). | HTTPS: The TLS Handshake Using Diffie-Hellman Ephemeral // THE CYBERSECURITY MAN: Интернет-портал. – URL: https://thecybersecurityman.com/2018/04/25/https-the-tls-handshake-using-diffie-hellman-ephemeral/ (дата обращения: 30.08.2020). |
|  | Спецификации ПО с открытым исходным кодом - Текст: электронный. – URL:  https://tools.ietf.org/ (дата обращения: 30.08.2020). |
|  | Безопасность протокола обмена ключами J-PAKE с аутентификацией паролем – Электронный ресурс. - URL: https://youtu.be/UHgXZWLcwd8 (дата обращения: 30.08.2020). |
|  | Что такое протокол безопасного удаленного пароля (SRP) и как его использовать? - Текст: электронный. – URL:  https://medium.com/swlh/what-is-secure-remote-password-srp-protocol-and-how-to-use-it-70e415b94a76 (дата обращения: 30.08.2020). |
|  | Разбираемся в повышении привилегий ОS Linux// Хабр: Интернет-портал. – URL: https://habr.com/ru/company/jetinfosystems/blog/505740/ (дата обращения: 30.08.2020). |
|  | Основы повышения привилегий Windows - Текст: электронный. – URL: http://www.fuzzysecurity.com/tutorials/16.html (дата обращения: 30.08.2020). |
|  | Цикл статей «Сети для самых маленьких» – Электронный ресурс. - URL: https://linkmeup.gitbook.io (дата обращения: 30.08.2020). |

**9.3. Материально-технические условия реализации программы**

|  |  |
| --- | --- |
| Вид занятий | Наименование оборудования,  программного обеспечения |
| Лекции | 1. ПК с операционной системой Linux, Windows или MacOs, удовлетворяющий системным требованиям платформы Moodle desktop.  2. Google Chrome или Firefox актуальных версий.  3. VirtualBox - среда виртуализации с открытым исходным кодом. Необходима для запуска виртуальных машин при выполнении лабораторных работ.  4. Ubuntu 20.04 desktop iso image - потребуется для выполнения лабораторных работ, если Linux не установлен в качестве основной ОС.  5. Kali Linux iso image - потребуется для выполнения лабораторных работ, если Kali Linux не установлен в качестве основной ОС.  6. Windows 10 iso image - потребуется для выполнения лабораторных работ, если Windows не установлен в качестве основной ОС.  7. Текстовый редактор - подойдет любой, например Sublime Text.  8. Nmap - средство сканирования сети с открытым исходным кодом. |
| Практические занятия | 1. ПК с операционной системой Linux, Windows или MacOs, удовлетворяющий системным требованиям платформы Moodle desktop.  2. Google Chrome или Firefox актуальных версий.  3. VirtualBox - среда виртуализации с открытым исходным кодом. Необходима для запуска виртуальных машин при выполнении лабораторных работ.  4. Ubuntu 20.04 desktop iso image - потребуется для выполнения лабораторных работ, если Linux не установлен в качестве основной ОС.  5. Kali Linux iso image - потребуется для выполнения лабораторных работ, если Kali Linux не установлен в качестве основной ОС.  6. Windows 10 iso image - потребуется для выполнения лабораторных работ, если Windows не установлен в качестве основной ОС.  7. Текстовый редактор - подойдет любой, например Sublime Text.  8. Nmap - средство сканирования сети с открытым исходным кодом. |
| Самостоятельная работа | 1. ПК с операционной системой Linux, Windows или MacOs, удовлетворяющий системным требованиям платформы Moodle desktop.  2. Google Chrome или Firefox актуальных версий.  3. VirtualBox - среда виртуализации с открытым исходным кодом. Необходима для запуска виртуальных машин при выполнении лабораторных работ.  4. Ubuntu 20.04 desktop iso image - потребуется для выполнения лабораторных работ, если Linux не установлен в качестве основной ОС.  5. Kali Linux iso image - потребуется для выполнения лабораторных работ, если Kali Linux не установлен в качестве основной ОС.  6. Windows 10 iso image - потребуется для выполнения лабораторных работ, если Windows не установлен в качестве основной ОС.  7. Текстовый редактор - подойдет любой, например Sublime Text.  8. Nmap - средство сканирования сети с открытым исходным кодом. |

**ПАСПОРТ КОМПЕТЕНЦИИ**

Основы безопасной веб-разработки

Автономная некоммерческая организация инновационного развития образования и науки «ФИРОН»

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Наименование компетенции | | Профессиональные компетенции необходимые при разработке и поддержке безопасных web-приложений для успешного выполнения профессиональных задач. | |
| 2. | Указание типа компетенции | общекультурная/  универсальная |  | |
| общепрофессиональная |  | |
| профессиональная |  | |
| профессионально-специализированная | + | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | | Слушатель должен иметь практический опыт в:  - использовании средств аудита безопасности;  - выявлении уязвимостей с использованием различных средств анализа защищенности;  - настройке систем безопасности web-приложений;  - выполнении разработки и проектирования информационных систем с учетом требований к уровню безопасности;  - модернизации веб-приложений с учетом требований к уровню безопасности. | |
| 4. | Дескриптор знаний, умений и навыков по уровням | | Уровни сформированности компетенции  обучающегося | Индикаторы |
|  | | Начальный уровень  (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.) | Владение основными методами, способами и средствами получения, хранения, переработки информации |
|  | | Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, сложности.) | Способность находить и определять уязвимости в web-приложениях, проводить аудит сетевой безопасности |
|  | | Продвинутый  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Способность  толковать нормативные правовые акты |
|  | | Профессиональный  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействующими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки  в ситуациях повышенной сложности.) | Способность составлять модель угроз информационной безопасности |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | Программа направлена на качественное изменение профессиональных компетенций, необходимых для выполнения вида профессиональной деятельности  «ВПД 1. Проектирование, разработка и оптимизация веб-приложений» в рамках имеющейся квалификации  ПК 1.1 Осуществлять аудит безопасности веб-приложения в соответствии с регламентами по безопасности;  ПК 1.2 Производить тестирование разработанного веб приложения;  ПК 1.3 Управлять доступом к данным и определять уровни прав пользователей ИР;  ПК 1.4 Обеспечивать безопасную и бесперебойную работу сайта;  ПК 1.5 Организовывать работы по обеспечению безопасной работы ИР. | |
| 6. | Средства и технологии оценки | | Уровень освоения знаний – тестирование;  Уровень освоения умений и навыков – тестирование, решение кейс-заданий | |

**VI.Иная информация о качестве и востребованности образовательной программы** (результаты профессионально-общественной аккредитации образовательной программы, включение в системы рейтингования, призовые места по результатам проведения конкурсов образовательных программ и др.) (при наличии)

**V.Рекомендаций к программе от работодателей**: наличие не менее двух писем и/или подтверждения на цифровой платформе Государственной системы предоставления ПЦС от работодателей о рекомендации образовательной программы для реализации в рамках Государственной системы предоставления ПЦС на формирование у трудоспособного населения компетенций цифровой экономики с указанием востребованности результатов освоения программы в сфере деятельности соответствующих компаний и готовности к рассмотрению заявок наиболее успешно освоивших образовательную программу граждан на прохождение стажировки и (или) собеседования на предмет трудоустройства путем проставления отметки в профиле программы

1. Письмо от ООО "НЦЗИ"

2. Письмо от ООО «Рнд Софт»

**VI. Указание на возможные сценарии профессиональной траектории граждан** по итогам освоения образовательной программы (в соответствии с приложением)

Развитие компетенций в текущей сфере занятости

**VII.Дополнительная информация**

**VIII. Приложенные Скан-копии**

Утвержденной рабочей программа (подпись, печать, в формате pdf)

**РУКОВОДИТЕЛЬ И СОСТАВИТЕЛИ ПРОГРАММЫ**

Руководитель образовательной программы

Директор АНО «ФИРОН» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Шенгоф И.С.

«23» октября 2020 г.