**Паспорт Образовательной программы**

**«**Методы несанкционированного доступа к информации

и противодействие им**»**

|  |  |
| --- | --- |
| 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 | Методы несанкционированного доступа к информации и противодействие им |
| 2.2 | Ссылка на страницу программы | <https://edu.firon.org/mod/forum/discuss.php?d=16> |
| 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) | 38 часов |
| 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://www.academyit.ru/courses/%D0%A2%D0%97%D0%9A%D0%98001/> 2. <https://mascom-uc.ru/events/m-3-0/> 3. <https://www.infosystems.ru/courses/kursy_soglasovannye_s_federalnymi_organami/obespechenie_bezopasnosti_personalnykh_dannykh_pri_ikh_obrabotke_v_informatsionnykh_sistemax_persona/> |
| 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 | Кибербезопасность и защита данных |

1. **Аннотация программы**

Онлайн-курс «Методы несанкционированного доступа к информации и противодействие им» поможет специалистам информационной безопасности сформировать навыки организации защиты информации.

Цель курса – сформировать у слушателей представление о многообразии способов несанкционированного доступа к информации и навыки противодействия им.

Задачи программы:

* изучение правовых основ и законодательства Российской Федерации;
* изучение требований регуляторов по защите конфиденциальной информации;
* подготовка к проведению аттестации объектов информатизации на соответствие требованиям по защите информации;
* изучение методов несанкционированного доступа к защищаемой информации с использованием технических средств и без них;
* изучение методов противодействия хакерским атакам.

Кадровое обеспечение программы осуществляет коллектив Общества с ограниченной ответственностью «Научный центр по защите информации» (ООО «НЦЗИ») и сотрудники Автономной некоммерческой организации «Фонд инновационного развития образования и науки» (АНО «ФИРОН»). Для повышения качества преподавания в рамках утверждённой программы к чтению лекций и итоговой аттестации могут привлекаться сотрудники организаций-партнеров.

Преподаватели курса – Инженеры ООО «НЦЗИ» (Научный центр по защите информации) Горбачев Андрей Викторович и Котенко Евгений Васильевич.

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**

|  |
| --- |
| «Методы несанкционированного доступа к информации  и противодействие им» |

(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**

Целью реализации программы повышения квалификации «Методы несанкционированного доступа к информации и противодействие им» является повышение осведомленности ответственных за защиту информации в организации в отношении методов и средств несанкционированного доступа к информации для последующего правильного определения угроз защищаемой информации и рационального использования средств при построении системы защиты конфиденциальной информации.

Программа имеет практическую направленность и базируется на изучении передового опыта в области защиты конфиденциальной информации.

**2. Планируемые результаты обучения:**

**2.1 Знание (осведомленность в областях)**

2.1.1. законодательство РФ в области защиты информации;

2.1.2. требования регуляторов по защите информации, не содержащей сведений, составляющих государственную тайну;

характеристики угроз безопасности информации.

* 1. **Умение (способность к деятельности)**

2.2.1. определять необходимый уровень защищенности информационной системы;

2.2.2. определять актуальные угрозы безопасности информации;

2.2.3. определять уязвимые места в системе защиты конфиденциальной информации

2.2.4. фиксировать атаки на информационную систему на этапе сбора информации о ней.

* 1. **Навыки (использование конкретных инструментов)**

2.3.1. построения эффективной системы защиты конфиденциальной информации;

2.3.2. восстановления удаленной информации с носителей;

2.3.3. использования возможностей специализированного программного обеспечения для тестирования информационной системы на проникновение.

**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 «Методы несанкционированного доступа к информации и противодействие им»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Модуль | Всего, час | Виды учебных занятий | | |
| лекции | практические занятия | самостоятельная работа |
| 1 | Модуль 1. Организации защиты конфиденциальной информации в соответствии с требованиями нормативно-правовых документов РФ | 18 | 11 | - | 6 |
| 2 | Модуль 2. Методы получения физического доступа к информации и противодействие им | 10 | 3 | 1 | 5 |
| 3 | Модуль 3. Социальная инженерия. Методы получения доступа к конфиденциальной информации | 11 | 17 | - | 3 |
| 4 | Модуль 4. Методы несанкционированного доступа к сетевому ресурсу (веб-серверу) | 31 | 7 | 6 | 17 |
| Итоговая аттестация | |  | 2 | | |
| тестирование | |  |  | | |

**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. Организации защиты конфиденциальной информации в соответствии с требованиями нормативно-правовых документов РФ | 18 | 1 - 3 ноября |
| 2 | Модуль 2. Методы получения физического доступа к информации и противодействие им | 10 | 4 - 6 ноября |
| 3 | Модуль 3. Социальная инженерия. Методы получения доступа к конфиденциальной информации | 11 | 7 - 9 ноября |
| 4 | Модуль 4. Методы несанкционированного доступа к сетевому ресурсу (веб-серверу) | 31 | 10-15 ноября |
|  | Итоговая аттестация | 2 | 15 ноября |
| Всего: | | 72 | 1-15 ноября |

**6. Учебно-тематический план программы «Методы несанкционированного доступа к информации и противодействие им»**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Модуль / Тема | Всего, час | Виды учебных занятий | | | Формы контроля |
| лекции | практические занятия | самостоятельная работа |  |
| 1 | **Модуль 1. Организации защиты конфиденциальной информации в соответствии с требованиями нормативно-правовых документов РФ** | 18 | 11 | - | 6 |  |
| 1.1 | Правовые и организационные основы защиты информации, не содержащей сведений, составляющих государственную тайну | 4 | 2 | - | 2 |  |
| 1.2 | Определение мероприятий по повышению эффективности защиты информации | 2 | 2 | - | - |  |
| 1.3 | Этапы создания системы защиты информации, рекомендации к классификации и категорированию объектов информатизации | 3 | 2 | - | 1 |  |
| 1.4 | Разработка модели угроз безопасности персональных данных | 4 | 2 | - | 2 |  |
| 1.5 | Содержание, порядок разработки и ввода в действие внутренних нормативных документов | 1 | 1 | - | - |  |
| 1.6 | Классификация и характеристика методов и средств защиты информации. Применение программно-аппаратных средств защиты информации | 2 | 1 | - | 1 |  |
| 1.7 | Содержание и порядок проведения аттестации объектов информатизации | 1 | 1 | - | - |  |
| 1.8 | **Промежуточная аттестация по Модулю 1** | 1 | - | - | - | тестирование |
| 2 | **Модуль 2. Методы получения физического доступа к информации и противодействие им** | 10 | 3 | 1 | 5 |  |
| 2.1 | Методы восстановления информации с устройств хранения информации | 4 | 1 | 1 | 2 |  |
| 2.2 | Методы перехвата информации с помощью специализированных устройств негласного съема информации | 3 | 1 | - | 2 |  |
| 2.3 | Методы противодействия получения физического доступа к информации | 2 | 1 | - | 1 |  |
| 2.4 | **Промежуточная аттестация по Модулю 2** | 1 | - | - | - | тестирование |
| 3 | **Модуль 3. Социальная инженерия. Методы получения доступа к конфиденциальной информации** | 11 | 7 | - | 3 |  |
| 3.1 | Введение в социальную инженерию | 2 | 1 | - | 1 |  |
| 3.2 | Психологические основы социальной инженерии | 2 | 1 | - | 1 |  |
| 3.3 | Этапы проведения атаки | 1 | 1 | - | - |  |
| 3.4 | Направления социальной инженерии | 1 | 1 | - | - |  |
| 3.5 | Использование вредоносного и специального программного обеспечения для проведения атаки | 2 | 1 | - | 1 |  |
| 3.6 | Социальная инженерия и тестирование на проникновение | 1 | 1 | - | - |  |
| 3.7 | Методы защиты от атак с использованием социальной инженерии | 1 | 1 | - | - |  |
| 3.8 | **Промежуточная аттестация по модулю 3** | 1 |  | - | - | тестирование |
| 4 | **Модуль 4. Методы несанкционированного доступа к сетевому ресурсу (веб-серверу)** | 31 | 7 | 6 |  |  |
| 4.1 | Обзор операционной системы Kali Linux | 1 | 1 | - | - |  |
| 4.2 | Развёртывание специализированной операционной системы для проведения атак на сетевой ресурс – Kali Linux | 4 | - | 1 | 3 |  |
| 4.3 | Знакомство с распространёнными командами Linux | 4 | 1 | 1 | 2 |  |
| 4.4 | Сбор информации об атакуемом сетевом ресурсе | 5 | 1 | 1 | 3 |  |
| 4.5 | Получение привилегий в операционной системе | 5 | 1 | 1 | 3 |  |
| 4.6 | Повышение привилегий | 5 | 1 | 1 | 3 |  |
| 4.7 | Доступ к защищаемой информации | 5 | 1 | 1 | 3 |  |
| 4.8 | Методы защиты от хакерских атак | 1 | 1 | - | - |  |
| 4.9 | **Промежуточная аттестация по Модулю 4** | **1** | - | - | - | **тестирование** |
| 5 | Итоговая аттестация | 2 | - | - | - | тестирование |
|  |  | 72 | 28 | 7 | 31 |  |

**7. Учебная (рабочая) программа повышения квалификации «Методы несанкционированного доступа к информации и противодействие им»**

**Модуль 1. Организации защиты конфиденциальной информации в соответствии с требованиями нормативно-правовых документов РФ (11 ак.ч.)**

Часть 1. (2 ак.ч.)

- рассмотрим нормативно-правовую базу документов по защите информации не содержащей сведений, составляющих государственную тайну.

Часть 2. (2 ак.ч.)

- будут рассмотрены организационные и технические меры защиты информации и их применение на том или ином объекте.

Часть 3. (2 ак.ч.)

- будут рассмотрены этапы создания системы защиты информации и рекомендации к классификации и категорированию объектов информатизации.

Часть 4. (2 ак.ч.)

- будет рассмотрена поэтапная разработка модели угроз, опираясь на такие документы как "Модель нарушителя ..." и "Банк данных угроз".

Часть 5. (1 ак.ч.)

- рассмотрим комплект организационно-распорядительной документации, который должен быть на каждом объекте информатизации.

Часть 6. (1 ак.ч.)

- рассмотрению подлежат программные и программно-аппаратные средства защиты информации, их характеристики, цели и задачи при защите информации на объекте информатизации.

Часть 7. (1 ак.ч.)

- раздел посвящен всем главным моментам, связанным с аттестацией объектов информатизации. При рассмотрении данного вопроса будем ссылаться на документ: "Положение по аттестации объектов информатизации по требованиям безопасности от 25 ноября 1994 года."

**Модуль 2. Методы получения физического доступа к информации и противодействие им (3 ак.ч.)**

Часть 1. (1 ак.ч.)

- технология хранения информации на запоминающих устройствах;

- программное обеспечение для восстановления информации с запоминающих устройств;

- пример атаки на информацию, хранящуюся в оперативной памяти.

Часть 2. (1 ак.ч.)

- виды технических каналов утечки информации;

- примеры технических средств негласного съема информации;

- технические средства негласного съема информации, доступные на рынке;

- ответственность за незаконный оборот технических средств негласного съема информации.

Часть 3. (1 ак.ч.)

- средства защиты информации от утечек по разным каналам утечки информации;

- основные программные средства защиты от физического доступа к защищаемой информации;

- основные средства криптографической защиты информации.

Часть 1. (1 ак.ч.)

- что такое социальная инженерия;

- современное применение социальной инженерии;

- социальная инженерия в информационной безопасности.

Часть 2. (1 ак.ч.)

- психология влияния;

- принципы влияния на людей.

Часть 3. (1 ак.ч.)

- основные этапы по осуществлению атаки с использованием социальной инженерии;

- описание каждого этапа.

Часть 4. (1 ак.ч.)

- современные направления социальной инженерии;

- примеры использования каждого направления социальной инженерии.

Часть 5. (1 ак.ч.)

- программное обеспечение, используемое при подготовке атаки;

- вредоносное программное обеспечение, используемое при атаках.

Часть 6. (1 ак.ч.)

- эффективность использования методов социальной инженерии при проведении тестирования на проникновение;

- примеры успешного применения социальной инженерии при проведении тестирования на проникновение.

Часть 7. (1 ак.ч.)

- методы защиты от атак, связанных с социальной инженерией;

- примеры использования защитных техник.

**Модуль 4. Методы несанкционированного доступа к сетевому ресурсу (веб-серверу) (7 ак.ч.)**

Часть 1. (1 ак.ч.)

- знакомство с операционной системой Kali Linux;

- знакомство с основными утилитами для атаки на сетевые ресурсы.

Часть 3. (1 ак.ч.)

- основные команды Linux, необходимые для тестирования на проникновение;

- дополнительные возможности командной строки Linux.

Часть 4. (1 ак.ч.)

- сбор информации об атакуемом хосте без использования специального программного обеспечения;

- сбор информации об атакуемом хосте с использованием специального программного обеспечения, предустановленного в операционной системе Kali Linux.

Часть 5. (1 ак.ч.)

- исследование атакуемого хоста на наличие уязвимостей;

- эксплуатация уязвимостей;

- получение пользовательских привилегий на атакуемом хосте.

Часть 6. (1 ак.ч.)

- исследование атакуемого хоста на наличие уязвимостей для повышения привилегий;

- основные методы повышения привилегий;

- эксплуатация уязвимостей для повышения привилегий;

- получение прав суперпользователя на атакуемом хосте.

Часть 7. (1 ак.ч.)

- исследование операционной системы с повышенными привилегиями;

- получение доступа к защищаемой информации;

- способы передачи защищаемой информации на атакующий хост;

- подготовка бэкдора;

- заметание следов.

Часть 8. (1 ак.ч.)

- основные средства защиты от сетевых атак;

- функционал средств защиты от сетевых атак;

- соответствие функционала средств защиты требованиям государственных регуляторов.

**Описание практико-ориентированных заданий и кейсов**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Номер темы/модуля | Наименование практического занятия | Описание |
| 1.1 | 1 | Ознакомление с основными организационно-распорядительными документами по защите информации, не содержащей сведений, составляющих государственную тайну | -знакомство и разбор нормативно-правовых документов |
| 1.2 | 1 | Ознакомление с государственными стандартами:  ГОСТ Р 50922 Защита информации. Основные термины и определения  ГОСТ Р 57628 Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности  ГОСТ Р ИСО/МЭК ТО 19791 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем  ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. | -знакомство и разбор представленных гос.стандартов |
| 2.1 | 1 | Разработка Модели угроз безопасности персональных данных | -описание информационной системы  -определение возможных источников атаки и реализации угроз безопасности информации  -проведение оценки актуальности нарушителя безопасности информации  -оценка актуальности угроз безопасности информации в соответствии с банком данных угроз ФСТЭК России |
| 2.2. | 1 | Ознакомление с основными сертифицированными средствами защиты информации.  Ознакомление со средствами защиты, представленными на официальных страницах производителей в сети Интернет. | Информация о средствах защиты информации расположена в реестре ФСТЭК России по адресу: https://fstec.ru/component/weblinks/?task=weblink.go&catid=6:uncategorised&id=5:reestr-sertifitsirovannykh-szi |
| 2.3 | 2 | Ознакомление с рынком программного обеспечения для восстановления данных.  Тестирование демоверсий программного обеспечения разных производителей. | - загрузка программного обеспечения различных производителей для восстановления удаленных файлов;  - ознакомление с интерфейсами программного обеспечения и его возможностями;  - тестирование функционала программного обеспечения путём удаления и восстановления файла на разных носителях информации. |
| 2.4 | 2 | Создание USB-накопителя для хищения информации с персонального компьютера | - загрузка программного обеспечения для автоматического сохранения защищаемых данных с компьютера;  - подготовка USB-носителя для атаки;  - тестирование функционала программного обеспечения |
| 2.5 | 2 | Разработка перечня мер защиты от физического доступа к защищаемой информации в организации | - ознакомление с функционалом средств защиты информации разных производителей;  - анализ актуальных угроз физического доступа в организации;  - составление перечня средств защиты информации, которые могут быть применены в организации. |
| 2.6. | 3 | Ознакомление с биографией и трудами Кевина Митника | - поиск в сети Интернет информации о биографии Кевина Митника;  - ознакомление с деятельностью К. Митника. |
| 2.7 | 3 | Разбор крупных кейсов | - анализ кейсов по использованию социальной инженерии в части использованных механизмов влияния |
| 2.8 | 3 | Ознакомление с подробным анализом нескольких экземпляров вредоносного ПО | - ознакомление с основными вирусами, используемыми в социальной инженерии;  - ознакомление с ущербом, нанесенным данными вирусами. |
| 2.9 | 4 | Знакомство с операционной системой и встроенными приложениями для проведения атак. Изучение их интерфейсов и функционала. | - установка виртуальной машины;  - загрузка операционной системы Kali Linux;  - развёртывание операционной системы Kali Linux;  - загрузка виртуальной машины для проведения атак;  - развёртывание виртуальной машины для проведения атак;  - настройка виртуальных машин для тестирования |
| 3.1 | 4 | Изучение дополнительных возможностей командной строки Linux. | - настройка командной строки;  - использование команд Linux |
| 3.2 | 4 | Сбор и протоколирование информации о сетевом ресурсе | - сбор информации об атакуемом хосте;  - протоколирование информации;  - знакомство с программным обеспечением, используемым для протоколирования. |
| 3.3 | 4 | Получение привилегий пользователя в операционной системе удалённого сетевого ресурса | - поиск уязвимостей тестовой системы;  - эксплуатация уязвимостей;  - получение пользовательских прав в системе |
| 3.4 | 4 | Повышение привилегий пользователя в операционной системе удалённого сетевого ресурса | - поиск уязвимостей и возможностей по повышению привилегий;  - эксплуатация уязвимостей;  - получение прав суперпользователя в тестовой системе. |
| 3.5 | 4 | Поиск и сохранение защищаемой информации. Создание бэкдора. Очистка следов пребывания на атакуемом хосте | - поиск и сохранение защищаемой информации;  - создание бэкдора;  - очистка следов пребывания на атакуемом хосте |

**8.Оценочные материалы по образовательной программе**

**8.1. Вопросы тестирования по модулям**

|  |  |  |  |
| --- | --- | --- | --- |
| № модуля | Вопросы входного тестирования | Вопросы промежуточного тестирования | Вопросы итогового тестирования |
| 1 | Оцените свои знания по современным методам и средствам защиты информации от несанкционированного доступа | 1. На основании какого документа проводится классификация ГИС?  a) ФЗ от 27.07.2006 № 152  b) Постановление Правительства РФ от 01.11.2012 № 1119  c) Приказ ФСТЭК России от  11 февраля 2013 г. № 17(правильный ответ)  d) Приказ ФСТЭК России от 18.02.2013 № 21  2. На какой срок выдаётся Аттестат соответствия требованиям безопасности информации для ИСПДн?  a)На весь срок эксплуатации информационной системы  b)На 3 года (правильный ответ)  c)На 5 лет  d)На 1 год  3. Сколько существует типов актуальных угроз для ИСПДн?  a)Один  b)Два  c)Три (правильный ответ)  d)Четыре  4. Какой документ определяет необходимый минимальный набор мер по защите информации, содержащейся в ИСПДн?  a)ФЗ от 27.07.2006 № 152  b)Постановление Правительства РФ от 01.11.2012 № 1119  c)Приказ ФСТЭК России от  11 февраля 2013 г. № 17  d)Приказ ФСТЭК России от 18.02.2013 № 21(правильный ответ)  5. Какой организационно-распорядительный документ определяет полномочия пользователя по доступу к ресурсам информационной системы?  a)Положение о разрешительной системе доступа (правильный ответ)  b)Технический паспорт  c)Описание технологического процесса обработки информации  d)Инструкция пользователя  6. Какое обязательное требование предъявляется к средствам защиты информации для их использования при создании системы защиты ИСПДн?  a)СЗИ должны пройти в установленном порядке процедуру оценки соответствия (правильный ответ)  b)СЗИ должны быть отечественного производства  c)СЗИ должны иметь открытый исходный код  7. Какой орган ведет реестр сертифицированных средств защиты информации?  a)ФСБ России  b)ФСТЭК России  c)Минобороны РФ  d)Все ответы верные(правильный ответ)  8. Как называется обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн?  a)Уровень защищенности ПДн  b)Класс защиты  c)Уровень исходной защищенности (правильный ответ)  d)Уровень доверия  9. Исходя из каких параметров информационной системы определяется класс защищенности ГИС?  a) Уровня значимости обрабатываемой информации и Масштаба информационной системы (правильный ответ)  b) Наличия подключения к другим информационным системам и Возможностям пользователя по доступу к информации  c) Количества используемых баз данных и Количества пользователей информационной системы  10. В каком случае не требуется брать у субъекта ПДн согласие на обработку ПДн?  a) Осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом  b)Обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах  c)Во всех указанных случаях (правильный ответ)  d)Обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных |  |
| 2 |  | 1. Как называется атака на сохраненную в оперативной памяти информацию при некорректном завершении работы операционной системы (отключении электропитания):  a) Rowhammer Attack  b) Safe Boot Attack  c) Cold Boot Attack (правильный ответ)  d) RAM Atack  2. Какая из перечисленных аббревиатур не относится к форматам файловой системы:  a) NTFS  b) FAT  c) MBR (правильный ответ)  d) EXT3  3. Как называется атака, заключающаяся в перепрошивке некоторых USB-устройств, с целью заставить устройство имитировать какое-то другое устройство (например флешка, имитирующая клавиатуру):  a) BadUSB (правильный ответ)  b) USBemul  c) USBcrack  d) HackUSB  4. В чем основное отличие «Быстрого» форматирования от «Полного»?  a) Быстрое форматирование не влияет на производительность системы  b) Быстрое форматирование восстанавливает повреждённые секторы диска  c) Быстрое форматирование продляет срок службы HDD  d) Быстрое форматирование фактически не удаляет данные с HDD (правильный ответ)  5. Возможно ли восстановить удалённые данные с SSD?  a) Да. Но только если данные были удалены в операционной системе Windows 7 и выше  b) Да. Но только если данные были удалены в операционной системе без поддержки команды TRIM (правильный ответ)  c) Нет  d) Да. Но только в течение ограниченного периода времени  6. Какой орган отвечает за сертификацию СКЗИ?  a) ФСБ России (правильный ответ)  b) ФСТЭК России  c) Роскомнадзор  d) Минкомсвязь России  7. Какой орган отвечает за сертификацию СЗИ от НСД?  a) ФСБ России  b) ФСТЭК России (правильный ответ)  c) Роскомнадзор  d) Минкомсвязь России  8. Как называет процедура по выявлению электронных устройств, предназначенных для негласного получения информации в технических средствах?  a) Специальные исследования  b) Специальная проверка (правильный ответ)  c) Специальное обследование  d) Сертификационные испытания |  |
| 3 |  | 1. Психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации – это …  a) Фишинг  b) Социальная инженерия (правильный ответ)  c) Вишинг  d) Фрикинг  2. Вид Интернет – мошенничества, при котором жертву заманивают на поддельный сайт для кражи учетных данных – это …  a) Фишинг (правильный ответ)  b) Социальная инженерия  c) Вишинг  d) Фрикинг  3. Атака, при которой мошенники, используя телефонную связь под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию или стимулируют к совершению определённых действий со своим карточным счетом, называется …  a) Фишинг  b) Социальная инженерия  c) Вишинг (правильный ответ)  d) Фрикинг  4. "Квид про кво" – это атака, в которой злоумышленник…  a) подкидывает жертве физический носитель информации с трояном  b) выуживает данные по заранее подготовленному сценарию  c) собирает информацию из мусора  d) создает ситуацию, когда жертва обратиться к нему за помощью (правильный ответ)  5. "Дорожное яблоко" – это атака, в которой злоумышленник…  a) подкидывает жертве физический носитель информации с трояном  b) собирает информацию из открытых источников  c) собирает информацию из мусора  d) создает ситуацию, когда жертва обратиться к нему за помощью (правильный ответ)  6. "Претекстинг" – это атака, в которой злоумышленник…  a) подкидывает жертве физический носитель информации с трояном  b) выуживает данные по заранее подготовленному сценарию (правильный ответ)  c) собирает информацию из мусора  d) создает ситуацию, когда жертва обратиться к нему за помощью  7. Самовоспроизводящийся программный код, который внедряется в установленные программы без согласия пользователя – это …  a) Вирус (правильный ответ)  b) Бэкдор  c) Троян  d) Руткит  8. Приложение, которое позволяет честному системному администратору или злобному злоумышленнику управлять вашим компьютером на расстоянии– это …  a) Вирус  b) Бэкдор (правильный ответ)  c) Троян  d) Руткит  9. Вредоносная программа, проникающая в компьютер под видом легитимного программного обеспечения – это …  a) Вирус  b) Бэкдор  c) Троян (правильный ответ)  d) Руткит  10. Вредоносная программа, проникающая в компьютер под видом легитимного программного обеспечения – это …  a) Вирус  b) Бэкдор  c) Троян (правильный ответ)  d) Руткит  11. Кейлогер – это …  a) компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему  b) программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя (правильный ответ)  c) программное обеспечение, показывающее рекламу  d) набор утилит для скрытия следов пребывания киберпреступников на зараженной машине, активности вредоносных программ и нежелательных либо потенциально опасных приложений  12. Эксплоит – это …  a) компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему пользователя (правильный ответ)  b) программное обеспечение или аппаратное устройство, регистрирующее различные действия  c) программное обеспечение, показывающее рекламу  d) набор утилит для скрытия следов пребывания киберпреступников на зараженной машине, активности вредоносных программ и нежелательных либо потенциально опасных приложений  13. Руткит – это …  a) компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему пользователя (правильный ответ)  b) программное обеспечение или аппаратное устройство, регистрирующее различные действия  c) программное обеспечение, показывающее рекламу  d) набор утилит для скрытия следов пребывания киберпреступников на зараженной машине, активности вредоносных программ и нежелательных либо потенциально опасных приложений |  |
| 4 |  | 1. Какое действие выполняет команда «man ls»:  a) Выводит список файлов в текущей директории  b) Запускает приложение ls от имени администратора  c) Выводит инструкцию по использованию приложения ls(правильный ответ)  d) Удалят файл ls в текущей директории  1. Какая команда запускает приложение от имени суперпользователя?  a) Sudo (правильный ответ)  b) ps  c) pwd  d) echo  2. Чего не хватает для успешного выполнения команды «cp /tmp/file.txt»?  a) Команда должна запускаться от имени суперпользователя  b) Не указан путь и имя файла для создания копии файла (правильный ответ)  c) В конце строки должен стоять символ «;»  3. Специальный идентификатор пользователя, позволяющий запускать файл от имени владельца файла  a) SGID  b) Sticky BIT  c) SUID (правильный ответ)  d) OUID  4. Посмотрите на скриншот. Где допущена ошибка?    a) Отсутствует сетевое подключение  b) Нет прав на запуск netcat  c) На сервере не указан параметр «с», определяющий номер порта для соединения (верхнее окно) (правильный ответ)  d) На клиенте не указан параметр «с», определяющий номер порта для соединения, (нижнее окно)  5. На хосте А запущена команда nc -l -p 3333 > fileA.txt. На хосте В запущена команда cat fileB.txt | nc -q 0 <hostA\_ip> 3333. Что произойдёт при завершении работы данных команд?  a) C хоста А на хост В будет передан файл fileA.txt с именем fileB.txt  b) Все команды, введенные в терминальном окне, на хосте В будут записаны на хосте А в файл fileA.txt  c) На хосте А и хосте В будут созданы два пустых файла fileA.txt и fileB.txt  d) На хост А будет передано содержимое файла fileB.txt и записано в файл fileA.txt(правильный ответ)  6. Для чего может быть использовано приложение NMAP  a) Для поиска уязвимостей на атакуемом хосте  b) Для сканирования хоста на наличие открытых портов для соединения (правильный ответ)  c) Для поиска возможных учетных записей для доступа к хосту  d) Для перебора паролей  7. Что такое Бэкдор?  a) Специально созданный механизм, позволяющий получить несанкционированный доступ к скомпрометированной операционной системе (правильный ответ)  b) Исправление программного обеспечения, которое закрывает определенную уязвимость операционной системы  c) Механизм восстановления удаленных злоумышленником данных  d) Механизм, позволяющий восстановить утерянный логин и пароль  8. Назовите основное отличие IDS и IPS  a) Нет отличий  b) IPS не может быть включен в разрыв защищаемой сети.  c) IDS сертифицируется ФСТЭК России, а IPS – ФСБ России  d) IDS только фиксирует наличие атаки, а IPS блокирует сетевой трафик с атакующего хоста (правильный ответ)  9. Какое решение позволяет выполнять фильтрацию трафика прикладного уровня, направленного на использование уязвимостей веб-серверов и приложений?  a) Web Application Firewall (правильный ответ)  b) Intrusion Prevention System.  c) Межсетевой экран  d) Антивирусное программное обеспечение |  |
| 5 |  |  | 1. Сколько существует уровней защищенности персональных данных?  a) Один  b) Два  c) Три  d)Четыре(правильный ответ)  2. Сколько существует классов защищенности государственных информационных систем?  a) Один  b) Два  c) Три (правильный ответ)  d) Четыре  3. На основании какого документа проводится определение необходимого уровня защищенности ПДн?  a) ФЗ от 27.07.2006 № 152  b) Постановление Правительства РФ от 01.11.2012 № 1119 (правильный ответ)  c) Приказ ФСТЭК России от  11 февраля 2013 г. № 17  d) Приказ ФСТЭК России от 18.02.2013 № 21  4. На какой срок выдаётся Аттестат соответствия требованиям безопасности информации для ГИС?  a) На весь срок эксплуатации информационной системы(правильный ответ)  b) На 3 года  c) На 5 лет  d) На 1 год  5. Для обеспечения максимальной надежности при удалении информации с жёсткого магнитного диска, без использования средств защиты информации, каким методом стоит воспользоваться?  a) Полное форматирование жёсткого диска (правильный ответ)  b) Быстрое форматирование жёсткого диска  c) Очистка корзины после удаления информации  d) Перезагрузка операционной системы для очистки остаточной информации, хранящейся в оперативной памяти  6. Какой из накопителей информации использует метод TRIM для очистки высвобождаемой памяти при удалении файлов?  a) SD карты  b) USB-Flash накопители  c) HDD  d) SSD (правильный ответ)  7. Программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя?  a) Руткит  b) Троян  c) Бэкдор  d)Кейлоггер(правильный ответ)  8. Как называется вид атаки, при которой пользователю отправляют ссылку на поддельный сайт, визуально похожий на оригинал, с целью получения его логина и пароля?  a) Фишинг (правильный ответ)  b) Вишинг  c) Квид про Кво  d) Претекстинг  9. Какой командой в операционной системе Linux можно вывести в командной строке содержимое файла?  a) ls  b) cat (правильный ответ)  c) cp  d) rm  10. Какое решение позволяет осуществлять блокировку трафика, содержащего сигнатуры атаки на сетевой ресурс?  a) IDS  b) WAF  c) IPS (правильный ответ)  d) FW |

**8.2.** Освоение слушателями программы повышения квалификации «Методы несанкционированного доступа к информации и противодействие им» завершается обязательной итоговой аттестацией, предусматривающей зачёт с оценкой в бальном эквиваленте, состоящий из последовательного выполнения четырех промежуточных онлайн-тестирований и итогового тестирования. В качестве оценочных средств освоения программы используются следующие виды:

* онлайн-тестирование по завершению изучения Модуля 1, максимальное количество баллов – 25;
* онлайн-тестирование по завершению изучения Модуля 2, максимальное количество баллов – 25;
* онлайн-тестирование по завершению изучения Модуля 3, максимальное количество баллов – 25;
* онлайн-тестирование по завершению изучения Модуля 4, максимальное количество баллов – 25;
* итоговое тестирование в целом по изученному материалу, максимальное количество баллов – 30.

При выполнении всех требований аттестации слушатель может заработать 130 баллов. К итоговой аттестации допускаются слушатели, набравшие не менее 50 баллов по итогам прохождения промежуточных тестов.

0-74 Незачет

75-100 Зачет

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

Примерные тестовые задания для проведения контроля знаний по Модулю 1 (тест). Максимальный бал за правильный ответ на каждый вопрос – 1 балла, за весь тест – не более 25 баллов:

1. На основании какого документа проводится классификация ГИС?

|  |  |
| --- | --- |
| 1. ФЗ от 27.07.2006 № 152 | 1. Постановление Правительства РФ от 01.11.2012 № 1119 |
| 1. Приказ ФСТЭК России от   11 февраля 2013 г. № 17(правильный ответ) | 1. Приказ ФСТЭК России от 18.02.2013 № 21 |

1. На какой срок выдаётся Аттестат соответствия требованиям безопасности информации для ИСПДн?

|  |  |
| --- | --- |
| 1. На весь срок эксплуатации информационной системы | 1. На 3 года (правильный ответ) |
| 1. На 5 лет | 1. На 1 год |

1. Сколько существует типов актуальных угроз для ИСПДн?

|  |  |
| --- | --- |
| 1. Один | 1. Два |
| 1. Три (правильный ответ) | 1. Четыре |

1. Какой документ определяет необходимый минимальный набор мер по защите информации, содержащейся в ИСПДн?

|  |  |
| --- | --- |
| 1. ФЗ от 27.07.2006 № 152 | 1. Постановление Правительства РФ от 01.11.2012 № 1119 |
| 1. Приказ ФСТЭК России от   11 февраля 2013 г. № 17 | 1. Приказ ФСТЭК России от 18.02.2013 № 21(правильный ответ) |

1. Какой организационно-распорядительный документ определяет полномочия пользователя по доступу к ресурсам информационной системы?

|  |  |
| --- | --- |
| 1. Положение о разрешительной системе доступа (правильный ответ) | 1. Технический паспорт |
| 1. Описание технологического процесса обработки информации | 1. Инструкция пользователя |

1. Какое обязательное требование предъявляется к средствам защиты информации для их использования при создании системы защиты ИСПДн?

|  |  |
| --- | --- |
| 1. СЗИ должны пройти в установленном порядке процедуру оценки соответствия (правильный ответ) | 1. СЗИ должны быть отечественного производства |
| 1. СЗИ должны иметь открытый исходный код |  |

1. Какой орган ведет реестр сертифицированных средств защиты информации?

|  |  |
| --- | --- |
| 1. ФСБ России | 1. ФСТЭК России |
| 1. Минобороны РФ | 1. Все ответы верные(правильный ответ) |

1. Как называется обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн?

|  |  |
| --- | --- |
| 1. Уровень защищенности ПДн | 1. Класс защиты |
| 1. Уровень исходной защищенности (правильный ответ) | 1. Уровень доверия |

1. Исходя из каких параметров информационной системы определяется класс защищенности ГИС?

|  |  |
| --- | --- |
| 1. Уровня значимости обрабатываемой информации и Масштаба информационной системы (правильный ответ) | 1. Наличия подключения к другим информационным системам и Возможностям пользователя по доступу к информации |
| 1. Количества используемых баз данных и Количества пользователей информационной системы |  |

1. В каком случае не требуется брать у субъекта ПДн согласие на обработку ПДн?

|  |  |
| --- | --- |
| 1. Осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом | 1. Обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах |
| 1. Во всех указанных случаях (правильный ответ) | 1. Обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных |

Примерные тестовые задания для проведения контроля знаний по Модулю 2 (тест). Максимальный бал за правильный ответ на каждый вопрос – 1 балл, за весь тест – не более 25 баллов:

1. Как называется атака на сохраненную в оперативной памяти информацию при некорректном завершении работы операционной системы (отключении электропитания):

|  |  |
| --- | --- |
| 1. Rowhammer Attack | 1. Safe Boot Attack |
| 1. Cold Boot Attack (правильный ответ) | 1. RAM Atack |

1. Какая из перечисленных аббревиатур не относится к форматам файловой системы:

|  |  |
| --- | --- |
| 1. NTFS | 1. FAT |
| 1. MBR (правильный ответ) | 1. EXT3 |

1. Как называется атака, заключающаяся в перепрошивке некоторых USB-устройств, с целью заставить устройство имитировать какое-то другое устройство (например флешка, имитирующая клавиатуру):

|  |  |
| --- | --- |
| 1. BadUSB (правильный ответ) | 1. USBemul |
| 1. USBcrack | 1. HackUSB |

1. В чем основное отличие «Быстрого» форматирования от «Полного»?

|  |  |
| --- | --- |
| 1. Быстрое форматирование не влияет на производительность системы | 1. Быстрое форматирование восстанавливает повреждённые секторы диска |
| 1. Быстрое форматирование продляет срок службы HDD | 1. Быстрое форматирование фактически не удаляет данные с HDD (правильный ответ) |

1. Возможно ли восстановить удалённые данные с SSD?

|  |  |
| --- | --- |
| 1. Да. Но только если данные были удалены в операционной системе Windows 7 и выше | 1. Да. Но только если данные были удалены в операционной системе без поддержки команды TRIM (правильный ответ) |
| 1. Нет | 1. Да. Но только в течение ограниченного периода времени |

1. Какой орган отвечает за сертификацию СКЗИ?

|  |  |
| --- | --- |
| 1. ФСБ России (правильный ответ) | 1. ФСТЭК России |
| 1. Роскомнадзор | 1. Минкомсвязь России |

1. Какой орган отвечает за сертификацию СЗИ от НСД?

|  |  |
| --- | --- |
| 1. ФСБ России | 1. ФСТЭК России (правильный ответ) |
| 1. Роскомнадзор | 1. Минкомсвязь России |

1. Как называет процедура по выявлению электронных устройств, предназначенных для негласного получения информации в технических средствах?

|  |  |
| --- | --- |
| 1. Специальные исследования | 1. Специальная проверка (правильный ответ) |
| 1. Специальное обследование | 1. Сертификационные испытания |

Примерные тестовые задания для проведения контроля знаний по Модулю 3 (тест). Максимальный бал за правильный ответ на каждый вопрос – 1 балл, за весь тест – не более 25 баллов:

1. Психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации – это …

|  |  |
| --- | --- |
| 1. Фишинг | 1. Социальная инженерия (правильный ответ) |
| 1. Вишинг | 1. Фрикинг |

1. Вид Интернет – мошенничества, при котором жертву заманивают на поддельный сайт для кражи учетных данных – это …

|  |  |
| --- | --- |
| 1. Фишинг (правильный ответ) | 1. Социальная инженерия |
| 1. Вишинг | 1. Фрикинг |

1. Атака, при которой мошенники, используя телефонную связь под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию или стимулируют к совершению определённых действий со своим карточным счетом, называется …

|  |  |
| --- | --- |
| 1. Фишинг | 1. Социальная инженерия |
| 1. Вишинг (правильный ответ) | 1. Фрикинг |

1. "Квид про кво" – это атака, в которой злоумышленник…

|  |  |
| --- | --- |
| 1. подкидывает жертве физический носитель информации с трояном | 1. выуживает данные по заранее подготовленному сценарию |
| 1. собирает информацию из мусора | 1. создает ситуацию, когда жертва обратиться к нему за помощью (правильный ответ) |

1. "Дорожное яблоко" – это атака, в которой злоумышленник…

|  |  |
| --- | --- |
| 1. подкидывает жертве физический носитель информации с трояном | 1. собирает информацию из открытых источников |
| 1. собирает информацию из мусора | 1. создает ситуацию, когда жертва обратиться к нему за помощью (правильный ответ) |

1. "Претекстинг" – это атака, в которой злоумышленник…

|  |  |
| --- | --- |
| 1. подкидывает жертве физический носитель информации с трояном | 1. выуживает данные по заранее подготовленному сценарию (правильный ответ) |
| 1. собирает информацию из мусора | 1. создает ситуацию, когда жертва обратиться к нему за помощью |

1. Самовоспроизводящийся программный код, который внедряется в установленные программы без согласия пользователя – это …

|  |  |
| --- | --- |
| 1. Вирус (правильный ответ) | 1. Бэкдор |
| 1. Троян | 1. Руткит |

1. Приложение, которое позволяет честному системному администратору или злобному злоумышленнику управлять вашим компьютером на расстоянии– это …

|  |  |
| --- | --- |
| 1. Вирус | 1. Бэкдор (правильный ответ) |
| 1. Троян | 1. Руткит |

1. Вредоносная программа, проникающая в компьютер под видом легитимного программного обеспечения – это …

|  |  |
| --- | --- |
| 1. Вирус | 1. Бэкдор |
| 1. Троян (правильный ответ) | 1. Руткит |

1. Вредоносная программа, проникающая в компьютер под видом легитимного программного обеспечения – это …

|  |  |
| --- | --- |
| 1. Вирус | 1. Бэкдор |
| 1. Троян (правильный ответ) | 1. Руткит |

1. Кейлогер – это …

|  |  |
| --- | --- |
| 1. компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему | 1. программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя (правильный ответ) |
| 1. программное обеспечение, показывающее рекламу | 1. набор утилит для скрытия следов пребывания киберпреступников на зараженной машине, активности вредоносных программ и нежелательных либо потенциально опасных приложений |

1. Эксплоит – это …

|  |  |
| --- | --- |
| 1. компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему пользователя (правильный ответ) | 1. программное обеспечение или аппаратное устройство, регистрирующее различные действия |
| 1. программное обеспечение, показывающее рекламу | 1. набор утилит для скрытия следов пребывания киберпреступников на зараженной машине, активности вредоносных программ и нежелательных либо потенциально опасных приложений |

1. Руткит – это …

|  |  |
| --- | --- |
| 1. компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему пользователя (правильный ответ) | 1. программное обеспечение или аппаратное устройство, регистрирующее различные действия |
| 1. программное обеспечение, показывающее рекламу | 1. набор утилит для скрытия следов пребывания киберпреступников на зараженной машине, активности вредоносных программ и нежелательных либо потенциально опасных приложений |

Примерные тестовые задания для проведения контроля знаний по Модулю 4 (тест). Максимальный бал за правильный ответ на каждый вопрос – 1 балла, за весь тест – не более 25 баллов:

1. Какое действие выполняет команда «man ls»:

|  |  |
| --- | --- |
| 1. Выводит список файлов в текущей директории | 1. Запускает приложение ls от имени администратора |
| 1. Выводит инструкцию по использованию приложения ls(правильный ответ) | 1. Удалят файл ls в текущей директории |

1. Какая команда запускает приложение от имени суперпользователя?

|  |  |
| --- | --- |
| 1. Sudo (правильный ответ) | 1. ps |
| 1. pwd | 1. echo |

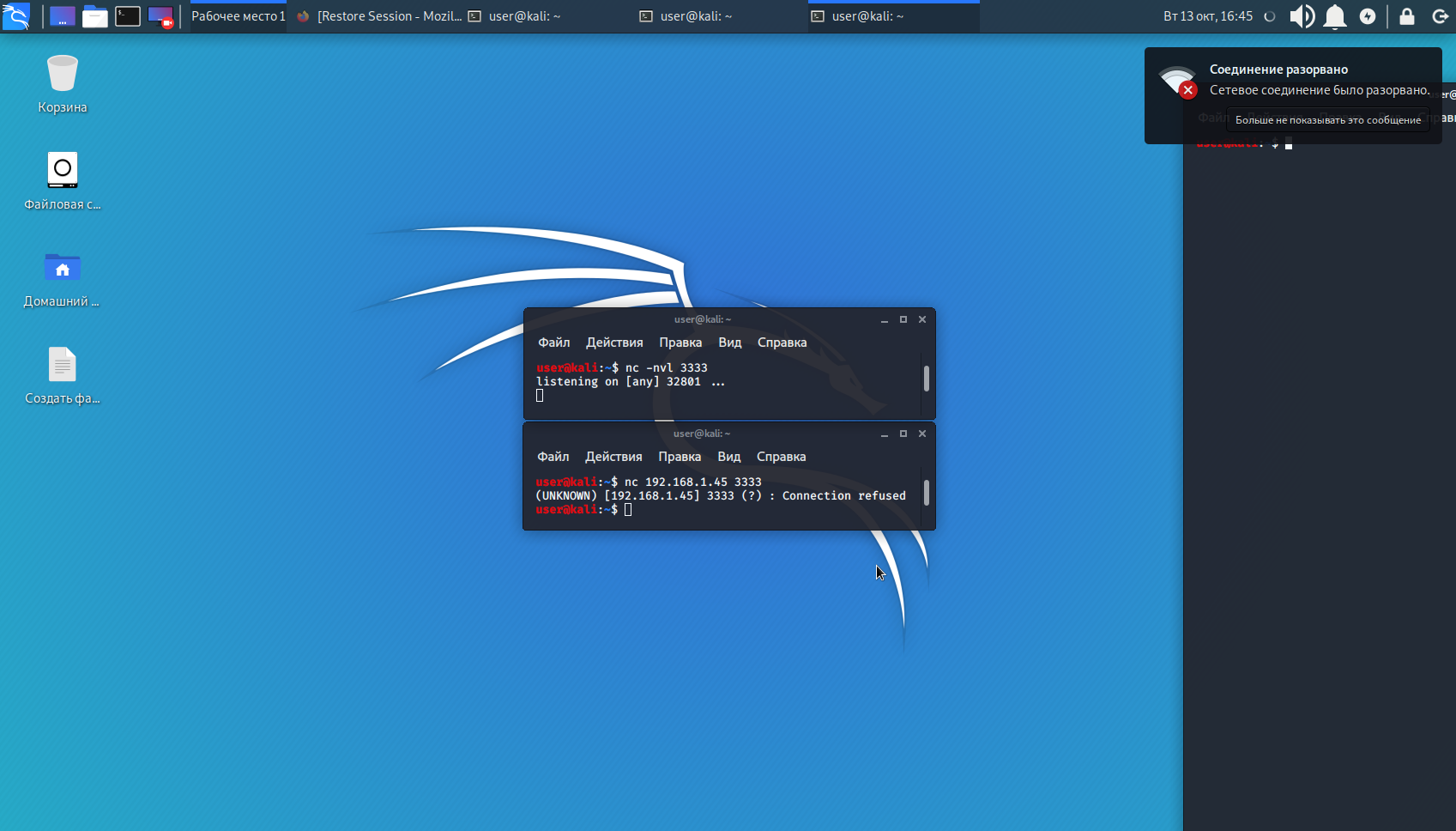
1. Чего не хватает для успешного выполнения команды «cp /tmp/file.txt»?

|  |  |
| --- | --- |
| 1. Команда должна запускаться от имени суперпользователя | 1. Не указан путь и имя файла для создания копии файла (правильный ответ) |
| 1. В конце строки должен стоять символ «;» |  |

1. Специальный идентификатор пользователя, позволяющий запускать файл от имени владельца файла

|  |  |
| --- | --- |
| 1. SGID | 1. Sticky BIT |
| 1. SUID (правильный ответ) | 1. OUID |

1. Посмотрите на скриншот. Где допущена ошибка?



|  |  |
| --- | --- |
| 1. Отсутствует сетевое подключение | 1. Нет прав на запуск netcat |
| 1. На сервере не указан параметр «с», определяющий номер порта для соединения (верхнее окно) (правильный ответ) | 1. На клиенте не указан параметр «с», определяющий номер порта для соединения, (нижнее окно) |

1. На хосте А запущена команда nc -l -p 3333 > fileA.txt. На хосте В запущена команда cat fileB.txt | nc -q 0 <hostA\_ip> 3333. Что произойдёт при завершении работы данных команд?

|  |  |
| --- | --- |
| 1. C хоста А на хост В будет передан файл fileA.txt с именем fileB.txt | 1. Все команды, введенные в терминальном окне, на хосте В будут записаны на хосте А в файл fileA.txt |
| 1. На хосте А и хосте В будут созданы два пустых файла fileA.txt и fileB.txt | 1. На хост А будет передано содержимое файла fileB.txt и записано в файл fileA.txt(правильный ответ) |

1. Для чего может быть использовано приложение NMAP

|  |  |
| --- | --- |
| 1. Для поиска уязвимостей на атакуемом хосте | 1. Для сканирования хоста на наличие открытых портов для соединения (правильный ответ) |
| 1. Для поиска возможных учетных записей для доступа к хосту | 1. Для перебора паролей |

1. Что такое Бэкдор?

|  |  |
| --- | --- |
| 1. Специально созданный механизм, позволяющий получить несанкционированный доступ к скомпрометированной операционной системе (правильный ответ) | 1. Исправление программного обеспечения, которое закрывает определенную уязвимость операционной системы |
| 1. Механизм восстановления удаленных злоумышленником данных | 1. Механизм, позволяющий восстановить утерянный логин и пароль |

1. Назовите основное отличие IDS и IPS

|  |  |
| --- | --- |
| 1. Нет отличий | 1. IPS не может быть включен в разрыв защищаемой сети. |
| 1. IDS сертифицируется ФСТЭК России, а IPS – ФСБ России | 1. IDS только фиксирует наличие атаки, а IPS блокирует сетевой трафик с атакующего хоста (правильный ответ) |

1. Какое решение позволяет выполнять фильтрацию трафика прикладного уровня, направленного на использование уязвимостей веб-серверов и приложений?

|  |  |
| --- | --- |
| 1. Web Application Firewall (правильный ответ) | 1. Intrusion Prevention System. |
| 1. Межсетевой экран | 1. Антивирусное программное обеспечение |

Примерные тестовые задания для проведения контроля знаний в целом по изученному материалу. Максимальный бал за правильный ответ на каждый вопрос – 1 балла, за весь тест – не более 25 баллов:

1. Сколько существует уровней защищенности персональных данных?

|  |  |
| --- | --- |
| 1. Один | 1. Два |
| 1. Три | 1. Четыре (правильный ответ) |

1. Сколько существует классов защищенности государственных информационных систем?

|  |  |
| --- | --- |
| 1. Один | 1. Два |
| 1. Три (правильный ответ) | 1. Четыре |

1. На основании какого документа проводится определение необходимого уровня защищенности ПДн?

|  |  |
| --- | --- |
| 1. ФЗ от 27.07.2006 № 152 | 1. Постановление Правительства РФ от 01.11.2012 № 1119 (правильный ответ) |
| 1. Приказ ФСТЭК России от   11 февраля 2013 г. № 17 | 1. Приказ ФСТЭК России от 18.02.2013 № 21 |

1. На какой срок выдаётся Аттестат соответствия требованиям безопасности информации для ГИС?

|  |  |
| --- | --- |
| 1. На весь срок эксплуатации информационной системы(правильный ответ) | 1. На 3 года |
| 1. На 5 лет | 1. На 1 год |

1. Для обеспечения максимальной надежности при удалении информации с жёсткого магнитного диска, без использования средств защиты информации, каким методом стоит воспользоваться?

|  |  |
| --- | --- |
| 1. Полное форматирование жёсткого диска (правильный ответ) | 1. Быстрое форматирование жёсткого диска |
| 1. Очистка корзины после удаления информации | 1. Перезагрузка операционной системы для очистки остаточной информации, хранящейся в оперативной памяти |

1. Какой из накопителей информации использует метод TRIM для очистки высвобождаемой памяти при удалении файлов?

|  |  |
| --- | --- |
| 1. SD карты | 1. USB-Flash накопители |
| 1. HDD | 1. SSD (правильный ответ) |

1. Программное обеспечение или аппаратное устройство, регистрирующее различные действия пользователя?

|  |  |
| --- | --- |
| 1. Руткит | 1. Троян |
| 1. Бэкдор | 1. Кейлоггер (правильный ответ) |

1. Как называется вид атаки, при которой пользователю отправляют ссылку на поддельный сайт, визуально похожий на оригинал, с целью получения его логина и пароля?

|  |  |
| --- | --- |
| 1. Фишинг (правильный ответ) | 1. Вишинг |
| 1. Квид про Кво | 1. Претекстинг |

1. Какой командой в операционной системе Linux можно вывести в командной строке содержимое файла?

|  |  |
| --- | --- |
| 1. ls | 1. cat (правильный ответ) |
| 1. cp | 1. rm |

1. Какое решение позволяет осуществлять блокировку трафика, содержащего сигнатуры атаки на сетевой ресурс?

|  |  |
| --- | --- |
| 1. IDS | 1. WAF |
| 1. IPS (правильный ответ) | 1. FW |

**8.4. Примерные практикоориентированные формы заданий**

- ознакомление с основными организационно-распорядительными документами по защите информации, не содержащей сведений, составляющих государственную тайну

- ознакомление с государственными стандартами:

ГОСТ Р 50922 Защита информации. Основные термины и определения

ГОСТ Р 57628 Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности

ГОСТ Р ИСО/МЭК ТО 19791 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем

ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения

- разработка Модели угроз безопасности персональных данных

- ознакомление с основными сертифицированными средствами защиты информации. Информация о средствах защиты информации расположена в реестре ФСТЭК России по адресу:

https://fstec.ru/component/weblinks/?task=weblink.go&catid=6:uncategorised&id=5:reestr-sertifitsirovannykh-szi

- ознакомление со средствами защиты, представленными на официальных страницах производителей в сети Интернет

- ознакомление с рынком программного обеспечения для восстановления данных. Тестирование демоверсий программного обеспечения разных производителей

- создание USB-накопителя для хищения информации с персонального компьютера

- разработка перечня мер защиты от физического доступа к защищаемой информации в организации**.**

**8.5.**  Измерительное испытание в начале обучения проводится в форме опроса об уровне знаний о современных методах и средствах защиты информации от несанкционированного доступа, промежуточные и итоговая аттестации проводятся в форме теста.

При подготовке к выполнению тестовых заданий обучающиеся используют весь учебный материал курса, источники основной и дополнительной литературы, ресурсы сети 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 правильный ответ. На выполнение тестов отводится не более 2 академических часов.

**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 | Котенко Евгений Васильевич | Инженер ООО «НЦЗИ» |  |  | + |
| 2 | Горбачев Андрей Викторович | Инженер ООО «НЦЗИ» |  |  | + |

**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. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».  2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».  3. Указ Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».  4. Постановление Правительства Российской Федерации от 01.11.2012  № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».  5. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».  6. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная заместителем директора ФСТЭК России 14.02.2008.  7. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная заместителем директора ФСТЭК России 15.02.2008.  8. «Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности», утвержденные руководством 8 Центра ФСБ России 31 марта 2015 года, № 149/7/2/6-432.  9. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», утвержденные приказом ФСБ России от 10 июля 2014 г. № 378.  10. ГОСТ Р 50922 «Защита информации. Основные термины и определения»  11. ГОСТ Р 57628 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности».  12. ГОСТ Р ИСО/МЭК ТО 19791 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем».  13. ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».  14. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».  15. Кузнецов, М. В. Социальная инженерия и социальные хакеры / М. В. Кузнецов, И. В. Симдянов. — СПб.: БХВ-Петербург, 2007.  16. Р. Чалдини. Психология влияния – СПб.: Прогресс-книга, 2020.  17. К. Митник, В. Саймон. Искусство вторжения – Москва. ДМК Пресс, 2005  18. К. Митник, В. Саймон. Призрак в Сети. Мемуары величайшего хакера – Москва. Эксмо, 2012 |

|  |  |
| --- | --- |
| Информационное сопровождение | |
| Электронные  образовательные ресурсы | Электронные  информационные ресурсы |
|  | Официальный сайт ФСТЭК России — <https://www.fstec.ru> |
|  | Habr — <https://www.habr.com> |
|  | Medium — <https://www.medium.com> |
|  | Cossa — [https://www.cossa.ru](https://www.cossa.ru/) |
|  | IT-Global — <https://itglobal.com/ru-ru/> |

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

|  |  |
| --- | --- |
| Вид занятий | Наименование оборудования,  программного обеспечения |
| Лекции | Оборудование и программы, необходимые для проведения вебинаров: компьютер c доступом в интернет, веб-камера, офисные программы, LMS Moodle  Операционная система – любая.  Любой современный браузер (например, Яндекс.Браузер, Google Chrome, Mozilla Firefox, Safari).  Поддерживаемые браузеры для работы LMS: (например, Yandex Browser 17+, Chrome 60+, Chrome Mobile 60+, Firefox 52+, Opera 50+) |
| Самостоятельная работа | Оборудование и программы, необходимые для проведения вебинаров: компьютер c доступом в интернет, веб-камера, офисные программы, LMS Moodle  Операционная система – любая.  Любой современный браузер (например, Яндекс.Браузер, Google Chrome, Mozilla Firefox, Safari).  Поддерживаемые браузеры для работы LMS: (например, Yandex Browser 17+, Chrome 60+, Chrome Mobile 60+, Firefox 52+, Opera 50+) |

**ПАСПОРТ КОМПЕТЕНЦИИ**

Методы несанкционированного доступа к информации и противодействие им

Автономная некоммерческая организация инновационного развития образования и науки «ФИРОН»

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Наименование компетенции | | Компетенции по направлению информационно безопасности | |
| 2. | Указание типа компетенции | общекультурная/  универсальная |  | |
| общепрофессиональная | + | |
| профессиональная |  | |
| профессионально-специализированная |  | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | | Программа направлена на получение знаний законодательства в области защиты персональных данных, получение практических навыков в области тестирования на проникновение. | |
| 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.) | Сформировано понимание многообразия способов несанкционированного доступа к информации |
|  | | Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, сложности.) | Освоены навыки организации системы защиты персональных данных с точки зрения законодательства |
|  | | Продвинутый  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Освоены навыки защиты от различных способов несанкционированного доступа к информации |
|  | | 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.) | Освоены навыки тестирования на проникновение |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | Компетенция информационной безопасности тесно связана с разработкой и сопровождением информационных систем. Наличие компетенции информационной безопасности желательно для разработчиков и администраторов информационных систем. | |
| 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, Переход в новую сферу 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.