1. **Паспорт Образовательной программы**

**«Сrash-курс по информационной безопасности»**

|  |  |
| --- | --- |
| **Версия программы** | **1** |
| **Дата Версии** | **08.10.2020** |

1. **Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | Университет Иннополис |
| 1.2 | Логотип образовательной организации |  |
| 1.3 | Провайдер ИНН | 1655258235 |
| 1.4 | Ответственный за программу ФИО | Бадрутдинова Гульгена Эдуардовна |
| 1.5 | Ответственный должность | менеджер проектов Университет Иннополиса |
| 1.6 | Ответственный Телефон | 89953315878 |
| 1.7 | Ответственный Е-mail | g.badrutdinova@innopolis.ru |

1. **Основные Данные**

|  |  |  |
| --- | --- | --- |
| **№** | **Название** | **Описание** |
| 2.1 | Название программы | Дополнительная профессиональная программа (программа повышения квалификации) “Crash-курс ” по информационной безопасности |
| 2.2 | Ссылка на страницу программы | <https://cdo-lms.innopolis.university/invite/XRAUR> |
| 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 | Подтверждаем |
| 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) | 61 академических часа:  Выполнение практических заданий - 26 часов  Выполнение самостоятельных работ - 35 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 | **15 000**  **Ссылки на аналогичные курсы:**   1. [**https://netology.ru/programs/informationsecurity**](https://netology.ru/programs/informationsecurity) 2. [**https://geekbrains.ru/geek\_university/security**](https://geekbrains.ru/geek_university/security) 3. [**https://skillbox.ru/course/profession-cybersecurity**](https://skillbox.ru/course/profession-cybersecurity) |
| 2.7 | Минимальное количество человек на курсе | **100** |
| 2.8 | Максимальное количество человек на курсе | **300** |
| 2.9 | Данные о количестве слушателей, ранее успешно прошедших обучение по образовательной программе | При наличии |
| 2.10 | Формы аттестации | зачет в форме контрольного тестирования |
|  | 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**

Программа регламентирует требования к повышению (расширению) квалификации в области кибербезопасности и защиты данных специалиста по информационной безопасности. Целью подготовки слушателей по Программе является совершенствование компетенций, необходимых для профессиональной деятельности специалиста по информационной безопасности. Учащиеся на данном курсе приобретают навыки работы с системами обнаружения вторжений, использования системы криптографической защиты информации, использования сетевых сканеров, перехвата и анализа сетевого трафика.

Результатами обучения на курсе являются:

Умение проводить собственные расследования инцидентов с помощью инструментария специалиста ИБ. Умение систематизировать знания в области оптимизации ИТ-инфраструктуры, организационных мер информационной безопасности, циклов безопасной разработки. Способность работать в компьютерных сетях с соблюдением действующих требований по защите информации. Устанавливать программное обеспечение в соответствии с технической документацией. Устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации. Применять средства защиты информации в компьютерных сетях,

используя основные сетевые технологии. Учебный процесс организуется с применением дистанционных образовательных технологий, инновационных технологий и методик обучения, способных обеспечить получение слушателями знаний, умений и навыков в области информационной безопасности. Программа повышения квалификации рассчитана на 72 академических часа. Лекционные и практические занятия проводятся в форме вебинаров. Задания и материалы программы размещаются в системе LMS Moodle, доступ к которой получают все обучающиеся.

Закрепление теоретического материала осуществляется через выполнение практических заданий с автоматизированной проверкой, тренажеров. К каждому занятию прилагается полный конспект, который загружается в платформу, что позволяет сделать изучение курса комфортным. Содержание вебинаров и практических заданий отличает высокая степень соответствия современному состоянию развития веб-технологий.

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ

ВЫСШЕГО ОБРАЗОВАНИЯ

«УНИВЕРСИТЕТ ИННОПОЛИС»

|  |  |
| --- | --- |
|  | **УТВЕРЖДЕНА**  Проректор – начальник управления по проектной и научно-исследовательской деятельности  АНО ВО «Университет Иннополис»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Бариев И.И.  Приказ № \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  от «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ г. |
|  |  |

**Дополнительная профессиональная программа**

**(программа повышения квалификации)**

|  |
| --- |
| **«Crash-курс по информационной безопасности»** |
| (наименование программы)  дополнительное профессиональное образование  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подвид дополнительного образования)  Иннополис 2020 г. |

**ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ**

**1.Цель программы**

Совершенствование компетенций, необходимых для профессиональной деятельности специалиста по информационной безопасности.

**2.Планируемые результаты обучения:**

2.1.Знание (осведомленность в областях)

2.1.1. уязвимости широко распространённых сетевых технологий и методы подавления таких уязвимостей;

2.1.2. типовые сетевые атаки и способы защиты от них;

2.1.3. сущность и содержание понятия ИБ, характеристики ее составляющей;

2.1.4. оценки рисков, виды рисков, методы управления рисками;

2.1..5. типовые kill chain;

2.1.6. общие принципы функционирования вредоносного программного обеспечения

2.1.7. сущность и содержание понятия информационной безопасности, характеристики ее составляющих

2.2. Умение (способность к деятельности)

2.2.1. проводить собственные расследования инцидентов с помощью инструментария специалиста ИБ;

2.2.2 проводить собственные расследования инцидентов с помощью инструментария специалиста ИБ;

2.2.3 систематизировать знания в области оптимизации ИТ-инфраструктуры, организационных мер информационной безопасности, циклов безопасной разработки;

2.2.4.работать в компьютерных сетях с соблюдением действующих требований по защите информации

2.2.5. устанавливать программное обеспечение в соответствии с технической документацией;

2.3.Навыки (использование конкретных инструментов)

2.3.1 применения средств защиты информации в компьютерных сетях;

2.3.2 использования основных сетевых технологий.

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

* 1. Лица, имеющие или получающие высшее или среднее профессиональное образование
  2. Разработчики ПО, специалисты по компьютерным сетям, системные администраторы, специалисты по информационной безопасности.
  3. релевантный опыт от 1 года.
  4. Предварительное освоение иных дисциплин/курсов /модулей

**4.Учебный план программы «Crash-курс по информационной безопасности»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль** | **Всего, час** | **Виды учебных занятий** | | |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| **1** | Основы защиты информации | **26** | **6** | **9** | **11** |
| **2** | Инструментарий специалиста ИБ | **42** | **1** | **17** | **24** |
| **Итоговая аттестация** | | **4** | **зачет** | | |

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

с 01.11.2020 – 16.11.2020 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** | Основы защиты информации | **26** | с 1.11.2020 - 6.11.2020 |
| **2** | Инструментарий специалиста ИБ | **42** | с 6.11.2020 - 15.11.2020 |
| **3** | Итоговая аттестация | **4** | 16.11.2020 |
| **Всего:** | | **72** |  |

**6. Учебно-тематический план программы «Crash-курс по информационной безопасности»**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль / Тема** | **Всего, час** | **Виды учебных занятий** | | | **Формы контроля** |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| **1** **.** | **Основы защиты информации** | **26** | **6** | **9** | **11** |  |
| 1.1. | Введение в информационную безопасность | 4 | 2 | 2 | 0 | **текущий** |
| 1.2. | Оценка рисков (качественная и количественная) | 4 | 1 | 3 | 0 | **текущий** |
| **1.3.** | Управление рисками | 4 | 1 | 1 | 2 | **текущий** |
| 1.4. | Основы защиты информационной инфраструктуры | 6 | 1 | 1 | 4 | **текущий** |
| 1.5. | Сетевые технологии | 8 | 1 | 2 | 5 | **текущий** |
| **2.** | **Инструментарий специалиста ИБ** | **42** | **1** | **17** | **24** | **текущий** |
| 2.1. | **Теория атак** | 22 | 0 | 8 | 14 | **текущий** |
| 2.2. | Инструментарий специалиста ИБ | 10 |  | 5 | 5 | **текущий** |
| 2.3. | Расследование инцидентов | 10 | 1 | 4 | 5 | **текущий** |
| **3.** | **Итоговая аттестация** | **4** |  |  |  | **зачет** |
|  | **Итого** |  |  |  |  |  |

**7. Учебная (рабочая) программа повышения квалификации**

**«Crash-курс по информационной безопасности »**

|  |  |  |
| --- | --- | --- |
| № п/п | Наименование и краткое содержание раздела | Объем, часов |
|  | **Модуль 1.** Основы защиты информации | **26** |
| 1.1 | Введение в информационную безопасность  *Краткое содержание:*  Обзор требований регуляторов и федеральных законов в части информационной безопасности. Документальное обеспечение безопасности информации. Основы базовой терминологии. Основные принципы информационной безопасности. Основные цели информационной безопасности. Границы информационной безопасности. | 4 |
| 1.2 | Оценка рисков (качественная и количественная)  *Краткое содержание:*  Применение различных подходов к оценке информационных рисков. Процесс анализа рисков. Необходимость и важность использования системы оценки и анализа рисков при проектировании системы обеспечения информационной безопасности | 4 |
| 1.3 | Управление рисками  *Краткое содержание:*  Основные системы анализа и оценки рисков. Современные методики управления рисками. Анализ (идентификация и измерение) риска. Критерии оценивания рисков информационной безопасности. Критерии принятия риска. Проведение непрерывного мониторинга и пересмотра рисков | 4 |
| 1.4 | Основы защиты информационной инфраструктуры  *Краткое содержание:*  Основные плюсы и минусы использования PKI. Цели применения криптографии в наши дни. Современные системы обеспечения защиты сетей и систем. Принципы построения защищенных систем связи;  требования национальных регуляторов в области. Навыки проектировки защищенных сетей и систем. Необходимые меры по обеспечению информационной безопасности сетей Защита данных во время хранения и транзита. Принципы методов аутентификации. Формирование защищенных каналов данных. | 6 |
| 1.5 | Сетевые технологии  *Краткое содержание:* Основные принципы работы сетевых технологий, базовых уязвимостей и атак на глобальные и локальные сети. Основы сетевых технологий. Классификация сетей передачи данных. Применение методов защиты от несанкционированного доступа в корпоративной сети. Модель взаимодействия открытых систем. Системы адресации используемые в сетевых технологиях | 8 |
|  | **Модуль 2.** Инструментарий специалиста ИБ | **42** |
| 2.1 | Теория атак  *Краткое содержание:*  Идентификация и обнаружение уязвимостей, угроз применение контрмер. Программные и системные ошибки. Вредоносное ПО. Принципы работы современных хакерских группировок. Применение базового инструментария для проверки защищенности инфраструктуры. Проведение пентеста. Сетевая безопасность. Управление доступом. Обеспечение непрерывности бизнес-процессов. Наиболее распространенные методы взлома. Комплексный поиск возможных методов доступа. Проведение пентеста. Сетевая безопасность. Управление доступом. Обеспечение непрерывности бизнес-процессов. Применение методов защиты от несанкционированного доступа в корпоративной сети. | 22 |
| 2.2 | Инструментарий специалиста ИБ  *Краткое содержание:*  Проведение тестирования на проникновение. Контроль и мониторинг информационной инфраструктуры. Предотвращение и реагирование на инциденты. Методы управления информационной безопасностью. Компетенции необходимые для начинающего специалиста. Назначение унификации и стандартизации. Состав базовых программных средств | 10 |
| 2.3 | Расследование инцидентов  *Краткое содержание:*  Формирование планов действий в случае чрезвычайных ситуаций и/или компрометации инфраструктуры. Поиск следов атак. Построение цепочки атак. Методы поиска вредоносного кода и атак на приложение. Инструменты, применяемые в расследовании. Этапы обработки инцидента информационной безопасности | 10 |
| 9. | Итоговая аттестация: Зачет в форме контрольного теститрования | **4** |

**Описание практико-ориентированных заданий и кейсов**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Номер темы/модуля | Наименование практического занятия | Описание |
|  | Модуль 1. Основы защиты информации | | |
| 1.1. | Введение в информационную безопасность | Тест-опрос «Введение в информационную безопасность» | ответить на вопросы по основным терминам |
| 1,2 | Оценка рисков (качественная и количественная) | Определить наименее рисковый проект. | выбор наиболее эффективных мер, для снижения рисков информационной  безопасности, учитывая  особенности методов управления рисками |
| 1.3 | Управление рисками | Выполнить Расчёт рисков и показателя возврата инвестиций при внедрении антивирусной системы. Построение виртуальной корпоративной сети; | выполнение оценки рисков, определение характеристик информационной системы, выполнение  анализа процедуры управления риском. Выполнение количественной оценки риска |
| 1.4 | Основы защиты информационной инфраструктуры | Разработка комплекса мер по защите информации в предприятии. | Обзор способов и протоколов аутентификации в веб-приложениях, учитывая системы и методы аутентификации пользователей. Обзор методов беспарольной аутентификации. Выявление критерии экспертной оценки применительно к системе информационной безопасности (ИБ) конкретной организации. |
|  |
| 1.5 | Сетевые технологии | Провести простейшую атаку на сетевые устройства. | Применить разные тактики, и подходы к атакам, стадии кибератаки при этом использовать различные виды сетевых атак. Рассмотреть основные уязвимости сетевых служб |
| 2 | Модуль 2 Инструментарий специалиста ИБ | | |
| 2.1 | Теория атак | Произвести исследование сервиса на наличие уязвимостей.Получить доступ к хостирующей машине. Найти флаг. | Выполнить описание объекта исследования. Выявить индикаторы компрометации для определения стадии атаки |
| 2.2 | Инструментарий специалиста ИБ | Провести проверку на наличие угроз | Провести нагрузочное тестирование сайта, развертывание системы мониторинга сервиса, развертывание системы управления логами, развертывание IDS. Провести проверку на наличие угроз, описать возможности, предоставляемые программой обнаружить хотя бы один вирус и описать его. |
| 2.3 | Расследование инцидентов | Построение таймлайна инцидента. | Необходимо найти первичную точку входа. Определить текущий этап атаки. Найти вредоносные файлы. Исследовать память на наличие чувствительной информации. |
| 3 | Итоговая аттестация | Материалы для контрольного тестирования в рамках итоговой аттестации | Выбрать верный из предложенных вариантов ответов контрольного теста |

**8.Оценочные материалы по образовательной программе**

**8.1. Вопросы тестирования по модулям**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ модуля** | **Вопросы входного тестирования** | **Вопросы промежуточного тестирования** | **Вопросы итогового тестирования** |
| 1. | оценивает уровень знаний слушателя, необходимый для освоения разделов Программы; (Приложение) | не предусмотрены программой | в форме зачета. Зачет в форме контрольного тестирования. Необходимо решить не менее 75% заданий контрольного теста |

**8.2.**  **описание показателей и критериев оценивания, шкалы оценивания** **.**

Тест-опрос «Введение в информационную безопасность»

* решено более 70 % от общего объема задач

Практические задания -

* Определен эффективный метод повышения безопасности информации, как с точки зрения быстродействия, так и с точки зрения точности.
* Сформулирован алгоритм обнаружения индикаторов компрометации данных.
* Оценено качество предложенного алгоритма действий и проведения сравнения эффективности различных алгоритмических решений

Итоговая аттестация-

* Решено не менее 75% заданий контрольного теста

**8.3. -8.5**  Перечень примерных практических заданий:

26.1 **Задание**: Тест-опрос «Введение в информационную безопасность»

1. Под информационной безопасностью понимается…

**А**) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.

Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия

В) нет правильного ответа

2. Защита информации – это..

**А)** комплекс мероприятий, направленных на обеспечение информационной безопасности.

Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей

В) небольшая программа для выполнения определенной задачи

3. От чего зависит информационная безопасность?

А) от компьютеров

**Б)** от поддерживающей инфраструктуры

В) от информации

4. Основные составляющие информационной безопасности:

**А**) целостность

**Б)** достоверность

**В)** конфиденциальность

5. Доступность – это…

**А)** возможность за приемлемое время получить требуемую информационную услугу.

Б) логическая независимость

В) нет правильного ответа

6. Целостность – это..

А) целостность информации

**Б)** непротиворечивость информации

**В)** защищенность от разрушения

7. Конфиденциальность – это..

**А)** защита от несанкционированного доступа к информации

Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

В) описание процедур

8. Для чего создаются информационные системы?

**А)** получения определенных информационных услуг

Б) обработки информации

В) все ответы правильные

9. Целостность можно подразделить:

**А**) статическую

**Б)** динамичную

В) структурную

10. Где применяются средства контроля динамической целостности?

**А)** анализе потока финансовых сообщений

Б) обработке данных

**В)** при выявлении кражи, дублирования отдельных сообщений

11.Какие трудности возникают в информационных системах при конфиденциальности?

А) сведения о технических каналах утечки информации являются закрытыми

Б) на пути пользовательской криптографии стоят многочисленные технические проблемы

**В)** все ответы правильные

12. Угроза – это…

**А)** потенциальная возможность определенным образом нарушить информационную безопасность

Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных

В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

13. Атака – это…

**А)** попытка реализации угрозы

Б) потенциальная возможность определенным образом нарушить информационную безопасность

В) программы, предназначенные для поиска необходимых программ.

14. Источник угрозы – это..

**А)** потенциальный злоумышленник

Б) злоумышленник

В) нет правильного ответа

15. Окно опасности – это…

**А)** промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.

Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области

В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

16. Какие события должны произойти за время существования окна опасности?

**А)** должно стать известно о средствах использования пробелов в защите.

**Б)** должны быть выпущены соответствующие заплаты.

**В)** заплаты должны быть установлены в защищаемой И.С.

17. Угрозы можно классифицировать по нескольким критериям:

**А)** по спектру И.Б.

**Б)** по способу осуществления

**В)** по компонентам И.С.

18. По каким компонентам классифицируется угрозы доступности:

**А**) отказ пользователей

**Б)** отказ поддерживающей инфраструктуры

В) ошибка в программе

19. Основными источниками внутренних отказов являются:

А) отступление от установленных правил эксплуатации

Б) разрушение данных

**В**) все ответы правильные

20. Основными источниками внутренних отказов являются:

**А)** ошибки при конфигурировании системы

Б) отказы программного или аппаратного обеспечения

В) выход системы из штатного режима эксплуатации

26.2 **Задание**

Пусть задано 3 инвестиционных проекта, данные по которым приведены в таблице. Определить наименее рисковый проект.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Проект | Прибыль, ден.ед. | Число случаев, n | Общее число случаев, N | Доля вероятности, Pi |
| А | 15  30  35  -20  -40 | 7  11  6  4  2 | 30  30  30  30  30 |  |
| Б | 65  45  20  -15  -25 |  |  | 0.2  0.4  0.1  0.2  0.1 |
| В | 50  30  15  -10  -20 | 10  15  20  10  5 | 60  60  60  60  60 |  |

26.3 **Задание:** Выполнить Расчёт рисков и показателя возврата инвестиций при внедрении антивирусной системы в банке на 10000 устройств. Построение виртуальной корпоративной сети.

**Требования**

Необходимо детальное рассмотрение процесса оценки рисков, определение характеристик информационной системы. Анализ процедуры управления риском. Количественная оценка риска. Современные методики управления рисками. Рассчитать SLE, ARO, ALE, ROI для предложенной ИС и выбранных рисков. Обосновать выбранные инструменты управления рисками расчётами ROI

26.4 **Задание:** Разработка комплекса мер по защите информации на предприятии.

**Требования:** Подсистема информационной безопасности должна содержать средства защиты КСПД, рабочих станций, периметра и мобильных устройств.

**Последовательность выполнения:**

• Обзор способов и протоколов аутентификации в веб-приложениях

• Обзор системы и методов аутентификации пользователей

• Обзор методов беспарольной аутентификации

• выявление критерии экспертной оценки применительно к системе информационной безопасности (ИБ) конкретной организации

26.5 **Задание: Провести простейшую атаку на сетевые устройства.**

**Последовательность выполнения:**

• построение DNS

• проведение анализа траффика в приложенном файле

• выполнение проектирования системы защиты корпоративной сети

• анализ сетевого траффика между рабочей станцией и сервером при авторизации по протоколу RDP при входе через доменное имя и по IP адресу.

26.6. **Задание:** Произвести исследование сервиса на наличие уязвимостей. Получить доступ к хостирующей машине. Найти флаг.

**Требования:** Необходимо разделиться на команды. Каждая команда запускает две виртуальных машины. Командам дается 2 дня на подготовительный этап для защиты веб службы. Затем необходимо атаковать сервис противоположной команды. Одновременно с этим необходимо обеспечить защищенность своего сервиса. Провести анализ лог-файлов. Провести анализ сетевого траффика. Провести анализ памяти, дампов памяти и свап-файлов. Произвести расследование инцидента. Сформировать базу данных трафика, содержащую информацию о риске безопасности или сведения об аномальном поведении пользователя в системе. Идентифицировать момент начала атаки и его окончание в операционной системе Windows.

26.7 **Задание: Провести проверку на наличие угроз**

Провести нагрузочное тестирование сайта, развертывание системы мониторинга сервиса, развертывание системы управления логами, развертывание IDS. Провести проверку на наличие угроз, описать возможности, предоставляемые программой обнаружить хотя бы один вирус и описать его.

**Требования**

Необходимо учитывать основные метрики для исследования на безопасность информации, технологию обнаружения проникновений, стратегии оповещения о тревогах с помощью инструментов.

26.8 **Задание:** Построение таймлайна инцидента.

Необходимо найти первичную точку входа. Определить текущий этап атаки. Найти вредоносные файлы. Исследовать память на наличие чувствительной информации.

**Требования.**

Необходимо применение новых функционалов. Использование на практике Timeline

**27. Материалы для контрольного тестирования в рамках итоговой аттестации:**

1. Как называется метод тестирования гипотез

a. market readiness;

b. null hypothesis;

c. custdev;

d. product pool.

2. Опубликованные исследования в сети Интернет это:

a. вторичные источники информации;

b. первичные источники информации;

c. сетевые источники информации;

d. свободные источники информации.

3.Что описывает модель OSI?

a. алгоритм кодирования-декодирования информации;

b. различные уровни взаимодействия открытых систем;

c. условное распределение оборудования по классам.

4.Какие функции выполняет DHCP-сервер?

a. возвращает имя хоста по IP адресу;

b. возвращает IP адрес по имени хоста;

c. пересылает электронные сообщения клиентам электронной почты;

d. динамически выдает IP адреса;

e. обрабатывает HTTP-запросы.

5. Отметьте уровни стека сетевых протоколов TCP/IP:

a. прикладной;

b. сеансовый;

c. канальный;

d. представления;

e. транспортный;

f. сетевой;

g. безопасный.

6. Выберите сети, которые не маршрутизируются в интернете:

a. 169.254.0.0;

b. 188.130.155.0;

c. 127.233.21.0;

d. 172.17.23.0;

e. 10.155.78.0;

f. 192.168.30.59;

g. 111.111.111.0.

7. Что содержит ARP-таблица?

a. сетевые адреса и соответствующие им порты маршрутизатора;

b. DNS записи;

c. сетевые адреса и соответствующие им физические адреса сетевых устройств;

d. физические адреса сетевых устройств и соответствующие им порты коммутатора.

8. Что такое MAC-адрес?

a. логический адрес сетевого устройства;

b. физический адрес сетевого устройства;

c. адрес сети;

d. адрес подсети;

e. адрес маски сети.

9. Что такое уязвимость нулевого дня?

a. уязвимость, которая известна всем;

b. уязвимость, о которой никто не знает;

c. известная уязвимость, исправление которой еще не разработано;

d. ни один из вышеперечисленных.

10. Безопасно ли использовать DES шифрование?

a. Безопасно;

b. безопасно, но только в локальных сетях;

c. безопасно, только при использовании ключа больше 256 бит;

d. не безопасно;

e. это не шифрование.

**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** | ***Иванов Илья Иванович*** |  |  |  |  |
|  |  |  |  |  |  |

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

|  |  |
| --- | --- |
| **Учебно-методические материалы** | |
| Методы, формы и технологии | Методические разработки,  материалы курса, учебная литература |
| · лекции;  · семинары (практические занятия);  · самостоятельная работа;  · итоговая аттестация (в форме зачета). | 1 Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов: Профобразование, 2019. — 702 c. — ISBN 978-5-4488-0070-2. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL:<http://www.iprbookshop.ru/87995.html>  2 Скрипник, Д.А. Общие вопросы технической защиты информации: учебное пособие / Д.А. Скрипник. — 3-е изд. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 424 c. — ISBN 978-5-4497-0336-1. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL:<http://www.iprbookshop.ru/89451.html>.  3 Фаронов, А.Е. Основы информационной безопасности при работе на компьютере: учебное пособие / А.Е. Фаронов. — 3-е изд. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 154 c. — ISBN 978-5-4497-0338-5. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL:<http://www.iprbookshop.ru/89453.html>. |
| Университет Иннополис обеспечен необходимым комплектом лицензионного программного обеспечения.  Каждый слушатель в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронно-библиотечной системе (электронной библиотеке) и к электронной информационно-образовательной среде Университета (https://my.university.innopolis.ru). Электронно-библиотечная система и электронная информационно-образовательная среда обеспечивают возможность доступа, слушателя из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»), как на территории Университета, так и вне ее.  Так же слушателям обеспечен доступ (удаленный доступ) к современным профессиональным базам данных и информационным справочным системам.  Для самостоятельной работы слушателей специальные помещения оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета. | |

|  |  |
| --- | --- |
| **Информационное сопровождение** | |
| Электронные  образовательные ресурсы | Электронные  информационные ресурсы |
| Лекции проводятся в формате онлайн вебинаров и видеолекций, размещенных на платформе университета LMC и доступных слушателям. Задания для самостоятельных работ размещаются также на платформе Университета. | |

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

|  |  |
| --- | --- |
| Вид занятий | Наименование оборудования,  программного обеспечения |
| *Университет располагает материально-технической базой, соответствующей действующим противопожарным правилам и нормам и обеспечивающей проведение всех видов дисциплинарной и междисциплинарной подготовки, практической и научно-исследовательской работ обучающихся, предусмотренных учебным планом;*  *Специальные помещения, которые представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского (практического) типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования укомплектованные специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории;*  *Для проведения занятий лекционного и семинарского (практического) типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие программе дисциплины (модуля).*  *Лаборатории Университета оснащены лабораторным и специализированным оборудованием.* | |

**III.Паспорт компетенций (Приложение 2)**

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ

ВЫСШЕГО ОБРАЗОВАНИЯ

«УНИВЕРСИТЕТ ИННОПОЛИС»

**ПАСПОРТ КОМПЕТЕНЦИИ**

Дополнительной профессиональная программа (программа повышения квалификации) «Crash-курс по информационной безопасности»

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Наименование компетенции | | Способностью понимать социальную значимость своей будущей профессии, обладать мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики | |
| 2. | Указание типа компетенции | (ОК - 5) | Общекультурная | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | | Под компетенцией ОК - 5 понимается осознание обучающимся сути и социальной значимости профессии, его готовность к осуществлению систематической деятельности по повышению профессионального мастерства. Стремление и готовность к совершению определенных поступков в целях удовлетворения профессиональных потребностей для достижения целей. | |
| 4. | Дескриптор знаний, умений и навыков по уровням | | Индикаторы | |
|  | **Необходимые знания:**  основополагающие термины и понятия; предметная область, цели, состав и значение информационных ресурсов организации; характеристики основных классов информационных технологий; базовые концепции корпоративных информационных систем; современное состояние отечественного ынка программного обеспечения корпоративных информационных систем  **Необходимые умения:**  самостоятельно изучать специальную литературу; проводить исследования в коммуникативном пространстве организации; оценивать эффективность коммуникаций в организации и анализировать причины их недостаточной эффективности; определять перспективные направления и пути совершенствования коммуникационной системы.  **Необходимые навыки:**  владеть навыками использования компьютерной техники и информационных технологий; владеть основами информационно-аналитической деятельности и способностью их применить в профессиональной сфере. | | Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределенности,сложности.) | Знать цели, задачи, принципы и основные направления обеспечения криптографической информационной безопасности государства;  Уметь проводить анализ и давать оценку степени защищенности компьютерных систем, осуществлять повышение уровня защиты с учетом криптографических средств защиты информации  Владеть профессиональной терминологией и методами теоретического обоснования в выборе криптографических средств обеспечения информационной безопасности. |
|
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | Перечислены основы для формирования компетенции ОК-5 :  ОПК-1:  способность анализировать физические явления и процессы для решения  профессиональных задач;  ОПК - 7  способность определять информационные ресурсы, подлежащие защите,  угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты  ПК-1:  Cпособность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации  ПК-2:  Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства для решения профессиональных задач | |
| 6. | Средства и технологии оценки | | * текущий контроль * итоговая аттестация | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Наименование компетенции | | ОПК-1:  способность анализировать физические явления и процессы для решения  профессиональных задач; | |
| 2. | Указание типа компетенции | общепрофессиональная |  | |
|  | Определение, содержание и основные сущностные характеристики компетенции | | Индикаторы | |
| 3. |  | |  | |
| 4. | Дескриптор знаний, умений и навыков по уровням | | Уровни сформированности компетенции  обучающегося | Индикаторы |
| **Необходимые знания:**  основные физические явления и законы, их описывающие;  - библиографические источники и информационно  -коммуникационные технологии для поиска необходимой информации;  - новые принципы построения систем моделирования;  - основные источники технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности  **Необходимые умения:**  - решать стандартные задачи;  - проводить научные исследования;  - решать задачи по физике на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий;  - применять на практике новые принципы систем моделирования;  - осуществлять подбор технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем.  **Необходимые навыки:**  - работы с библиографическими источниками; - проведения научно - исследовательской работы;  - работы с библиографическими источниками и информационно- коммуникационными технологиями;  - физико-математическим аппаратом для решения задач профессиональной деятельности;  - навыками применения новых технологий моделирования инфокоммуникационных систем и сетей;  - начальными навыками подбора, изучения, анализа и обобщения научно-технической информации, нормативных и методических материалов. | | Базовый уровень  Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, сложности. | Знать основные физические явления и законы, библиографические источники и информационно-коммуникационные технологии для поиска необходимой информации, основные источники технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности  Уметь решать стандартные задачи;  - проводить научные исследования;  - решать задачи по физике на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий;  - применять на практике новые принципы систем моделирования;  - осуществлять подбор технической информации, нормативных и методических материалов по методам обеспечения информационной безопасности телекоммуникационных систем.  Иметь навыки :  работы с библиографическими источниками; - проведения научно - исследовательской работы;  - работы с библиографическими источниками и информационно- коммуникационными технологиями;  - физико-математическим аппаратом для решения задач профессиональной деятельности;  - навыками применения новых технологий моделирования инфокоммуникационных систем и сетей;  - начальными навыками подбора, изучения, анализа и обобщения научно-технической информации, нормативных и методических материалов. |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | Перечислены основы для формирования компетенции ОПК-1 :  ОК - 5  способностью понимать социальную значимость своей будущей профессии, обладать мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики  ОПК - 7  способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты  ПК-1:  способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации  ПК-2:  способность применять программные средства системного, прикладного и специального назначения, инструментальные средства для решения профессиональных задач | |
| 6. | Средства и технологии оценки | | * текущий контроль * итоговая аттестация | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Наименование компетенции | | ОПК-7:  способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты | |
| 2. | Указание типа компетенции | общепрофессиональная |  | |
|  | Определение, содержание и основные сущностные характеристики компетенции | | Индикаторы | |
| 3. |  | |  | |
| 4. | Дескриптор знаний, умений и навыков по уровням | | Уровни сформированности компетенции  обучающегося | Индикаторы |
| **Необходимые знания:**  основные концепции и архитектуры построения систем управления информационной безопасностью;  **Необходимые умения:**   * проводить аудит и анализировать состояние информационной безопасности на объектах информатизации и в организациях, использующих в своей деятельности информационные системы   **Необходимые навыки:**  иметь представление о существующих и перспективных продуктах управления системами информационной безопасности. | | Базовый уровень  Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределенности, сложности. | Знать основные концепции и архитектуры построения систем управления информационной безопасностью;  Уметь проводить аудит и анализировать состояние информационной безопасности на объектах информатизации и в организациях, использующих в своей деятельности информационные системы  Иметь навыки :  представления о существующих и перспективных продуктах управления системами информационной безопасности. |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | Перечислены основы для формирования компетенции ОПК-7 :  ОК - 5  способностью понимать социальную значимость своей будущей профессии, обладать мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики  ОПК-1:  способность анализировать физические явления и процессы для решения  профессиональных задач;  ПК-1:  способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации  ПК-2:  способность применять программные средства системного, прикладного и специального назначения, инструментальные средства для решения профессиональных задач | |
| 6. | Средства и технологии оценки | | * текущий контроль * итоговая аттестация | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Наименование компетенции | | ПК-1:  способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации | |
| 2. | Указание типа компетенции | профессиональная |  | |
|  | Определение, содержание и основные сущностные характеристики компетенции | | Индикаторы | |
| 3. |  | |  | |
| 4. | Дескриптор знаний, умений и навыков по уровням | | Уровни сформированности компетенции  обучающегося | Индикаторы |
| **Необходимые знания:**   |  | | --- | | · Типовые сетевые атаки и способы защиты от них |   Сущность и содержание понятия ИБ,  характеристики ее составляющей  **Необходимые умения:**   * - применять программно-аппаратные средства защиты информации в компьютерных сетях * - работать в компьютерных сетях с соблюдением действующих требований по защите информации   **Необходимые навыки:**  иметь представление о существующих и перспективных продуктах управления системами информационной безопасности. | | Базовый уровень  Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределенности, сложности. | Знать:  типовые сетевые атаки и способы защиты от них на базовом уровне  сущность и содержание понятия ИБ, характеристики ее составляющей на базовом уровне  Уметь:  применять программно-аппаратные средства защиты информации в компьютерных сетях  работать в компьютерных сетях с соблюдением действующих требований по защите информации  сравнивать технико-эксплуатационные возможности устройств и систем защиты информации на базовом уровне  Иметь навыки :  представления о существующих и перспективных продуктах управления системами информационной безопасности;  использования программно-аппаратных средств защиты информации в профессиональной деятельности на базовом уровне |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | Перечислены основы для формирования компетенции ПК-1 :  ОК - 5  способностью понимать социальную значимость своей будущей профессии, обладать мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики  ОПК-1:  способность анализировать физические явления и процессы для решения  профессиональных задач;  ОПК - 7  способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты  ПК-2:  способность применять программные средства системного, прикладного и специального назначения, инструментальные средства для решения профессиональных задач | |
| 6. | Средства и технологии оценки | | * текущий контроль * итоговая аттестация | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Наименование компетенции | | ПК-2:  способность применять программные средства системного, прикладного и специального назначения, инструментальные средства для решения профессиональных задач | |
| 2. | Указание типа компетенции | профессиональная |  | |
|  | Определение, содержание и основные сущностные характеристики компетенции | | Индикаторы | |
| 3. |  | |  | |
| 4. | Дескриптор знаний, умений и навыков по уровням | | Уровни сформированности компетенции  обучающегося | Индикаторы |
| **Необходимые знания:**•  - общие принципы функционирования вредоносного программного обеспечения  - сущность и содержание понятия информационной безопасности, характеристики ее составляющих  **Необходимые умения:**   * - устанавливать программное обеспечение в соответствии с технической документацией * - устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации   **Необходимые навыки:**  - применения средств защиты информации в компьютерных сетях  -использования основных сетевых технологий. | | Базовый уровень  Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределенности, сложности. | Знать:  общие принципы функционирования вредоносного программного обеспечения на базовом уровне  - сущность и содержание понятия информационной безопасности, характеристики ее составляющих на базовом уровне  Уметь:  - устанавливать программное обеспечение в соответствии с технической документацией на базовом уровне   * - устанавливать обновления программного обеспечения, включая программное обеспечение средств защиты информации на базовом уровне   Иметь навыки :  применения средств защиты информации в компьютерных сетях на базовом уровне  -использования основных сетевых технологий на базовом уровне |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | Перечислены основы для формирования компетенции ПК-2 :  ОК - 5  способностью понимать социальную значимость своей будущей профессии, обладать мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики  ОПК-1:  способность анализировать физические явления и процессы для решения  профессиональных задач;  ОПК - 7  способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты  ПК-1:  способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации | |
| 6. | Средства и технологии оценки | | * текущий контроль * итоговая аттестация | |

**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

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

**Приложенные Скан-копии**

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