**МИНИCTEPCTBO НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ**

**РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное автономное образовательное учреждение высшего образования**

**«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**

«УТВЕРЖДАЮ»

и.о. проректора по учебной работе,

заместитель проректора

Мезенцева О.С.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_2020 г.

**Паспорт дополнительной профессиональной программы**

**повышения квалификации**

**«Менеджмент инцидентов кибербезопасности»**

|  |  |  |
| --- | --- | --- |
| Объём занятий: | Всего: | - 72 часа |
|  | в.т.ч.: лекций | - 20 часов |
|  | практические занятия | - 38 часов |
|  | самостоятельная работа | - 10 часов |
|  | Тестирование | - 2 часа |

|  |  |
| --- | --- |
|  | РАЗРАБОТАНО  Руководитель программы    \_\_\_\_\_\_\_\_\_\_\_ Огур М.Г.  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2020 г. |

Ставрополь, 2020 г

**«Менеджмент инцидентов кибербезопасности»**

|  |  |
| --- | --- |
| **Версия программы** | **1** |
| **Дата Версии** | **14.10.2020** |

1. **Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | **ФГАОУ ВО «Северо-Кавказский федеральный университет»** |
| 1.2 | Логотип образовательной организации |  |
| 1.3 | Провайдер ИНН | **2635014955** |
| 1.4 | Ответственный за программу ФИО | **Огур Максим Геннадьевич** |
| 1.5 | Ответственный должность | **Старший преподаватель кафедры прикладной математики и компьютерной безопасности института математики и информационных технологий имени профессора Н.И. Червякова Северо-Кавказского федерального университета** |
| 1.6 | Ответственный Телефон | **+79887091810** |
| 1.7 | Ответственный Е-mail | [**mogur@ncfu.ru**](mailto:mogur@ncfu.ru)  **ogur26@gmail.com** |

1. **Основные Данные**

|  |  |  |
| --- | --- | --- |
| **№** | **Название** | **Описание** |
| 2.1 | Название программы | **Менеджмент инцидентов кибербезопасности** |
| 2.2 | Ссылка на страницу программы | [**https://el.ncfu.ru/course/view.php?id=1412**](https://el.ncfu.ru/course/view.php?id=1412)  [**https://www.ncfu.ru/education/dop-prof/proekt-cifrovoi-sertifikat/Menedjment-incidentov-kiberbezopasnosti/#**](https://www.ncfu.ru/education/dop-prof/proekt-cifrovoi-sertifikat/Menedjment-incidentov-kiberbezopasnosti/#)  [**https://www.ncfu.ru/education/dop-prof/proekt-cifrovoi-sertifikat/**](https://www.ncfu.ru/education/dop-prof/proekt-cifrovoi-sertifikat/) |
| 2.3 | Формат обучения | **Онлайн** |
| 2.4 | 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 | **Есть** |
| 2.5 | Уровень сложности | **Базовый/Продвинутый** |
| 2.6 | Количество академических часов | **72** |
| 2.7 | 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 выделено на выполнение практических и семинарских занятий,**  **10 часов выделено на выполнение практических заданий в режиме самостоятельной работы.** |
| 2.8 | 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 (тридцать тысяч ) рублей 00 коп.**  **Аналогичные программы:**  [**https://itsecurity.ru/catalog/bt41/**](https://itsecurity.ru/catalog/bt41/) (24 ак. часа, стоимость 32500 руб)  [**http://www.cprspb.ru/pages/2020/ppk7ars.html**](http://www.cprspb.ru/pages/2020/ppk7ars.html)  [**https://www.academyit.ru/courses/%D0%98%D0%91040/**](https://www.academyit.ru/courses/%D0%98%D0%91040/)(40 часов, стоимость 57900 руб)  [**https://www.group-ib.ru/landing/incident-response-workshop.html?utm\_source=banner&utm\_medium=banner&utm\_campaign=ir**](https://www.group-ib.ru/landing/incident-response-workshop.html?utm_source=banner&utm_medium=banner&utm_campaign=ir)(12 часов, стоимость 36000 руб) |
| 2.9 | Минимальное количество человек на курсе | **1** |
| 2.10 | Максимальное количество человек на курсе | **300** |
| 2.11 | Данные о количестве слушателей, ранее успешно прошедших обучение по образовательной программе | **Программа на платформе 20.35 реализуется впервые**  **Очное обучение по аналогичной программе у провайдера ФГАОУ ВО «Северо-Кавказский федеральный университет» прошли более 20 человек.** |
| 2.12 | Формы аттестации | **Компьютерное тестирование** |
| 2.13 | 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**

«Менеджмент инцидентов кибербезопасности» – практико-ориентированная дополнительная профессиональная программа повышения квалификации, нацелена на формирование практических умений, навыков и (или) приобретение опыта, необходимого для выполнения вида профессиональной деятельности №06.032 «Защита информации в компьютерных системах и сетях», конкретного самостоятельного вида деятельности при соответствии требованиям работодателя, либо осуществление работы по укрупненной группе специальностей «Информационная безопасность» наряду с основным видом деятельности в области цифровой экономики и соответствует области «Кибербезопасность и защита данных».

Программа соответствует действующему законодательству РФ (Федеральному закону «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ (актуальная редакция), Приказу Министерства образования и науки Российской Федерации (Минобрнауки России) от 1 июля 2013 г. № 499 г. Москва «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам», Приказом Министерства образования и науки РФ от 23 августа 2017 г. № 816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»).

Программа соответствует профессиональному стандарту №842 «Специалист по безопасности компьютерных систем и сетей».

Модуль 1 – разработка и документирование политики менеджмента инцидентов кибербезопасности.

Модуль 2 – формы, процедуры и инструменты поддержки обнаружения, оповещения, оценки и реагирования на инциденты кибербезопасности.

Модуль 3 – обновление политик менеджмента информационной безопасности и рисков на всех уровнях, то есть на корпоративном и для каждой системы, сервиса и сети отдельно с учетом системы менеджмента инцидентов кибербезопасности.

Модуль 4 – обнаружение и оповещение о возникновении событий кибербезопасности (человеком или автоматическими средствами).

Модуль 5 – сбор информации, связанной с событиями кибербезопасности, оценка этой информации с целью отнесения к категории инцидентов кибербезопасности.

Модуль 6 – способы реагирования на инциденты кибербезопасности.

**Цель реализации программы**

Целью реализации программы является комплексное обновление знаний по информационным и цифровым технологиям, необходимым в профессиональной деятельности, прочное усвоение слушателями фундаментальных основ и принципов общей стратегии кибербезопасности, в рамках которой необходимо использовать структурный подход к менеджменту инцидентов, практики применения данных технологий, а также совершенствование умений и навыков слушателей с учетом специализации их профессиональной деятельности, повышения профессионального уровня в рамках имеющейся квалификации.

**Требования к уровню образования и (или) квалификации обучающегося:**

Необходимо наличие среднего профессионального или высшего образования по группам направлений и специальностей из списка:

* 02.00.00 – Компьютерные и информационные науки;
* 09.00.00 – Информатика и вычислительная техника;
* 10.00.00 – Информационная безопасность.

**МИНИCTEPCTBO НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ**

**РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное автономное образовательное учреждение высшего образования**

**«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**

«УТВЕРЖДАЮ»

и.о. проректора по учебной работе

Мезенцева О.С.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

«\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_2020 г.

**Дополнительная профессиональная программа**

**повышения квалификации**

**«Менеджмент инцидентов кибербезопасности»**

|  |  |  |
| --- | --- | --- |
| Объём занятий: | Всего: | - 72 часа |
|  | в т.ч.: лекций | - 20 часов |
|  | практические занятия | - 38 часов |
|  | самостоятельная работа | - 10 часов |
|  | Тестирование | - 2 часа |

|  |  |
| --- | --- |
| СОГЛАСОВАНО  Зав. кафедрой прикладной математики и компьютерной безопасности  \_\_\_\_\_\_\_\_\_\_\_\_\_ Тебуева Ф.Б.  «\_\_\_»\_\_\_\_\_\_\_\_\_\_ 2020 г. | РАЗРАБОТАНО  Руководитель программы    \_\_\_\_\_\_\_\_\_\_\_ Огур М.Г.  «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2020 г. |

СОГЛАСОВАНО

И.о. директора института математики

и информационных технологий

имени профессора Н.И. Червякова

\_\_\_\_\_\_\_\_\_\_\_\_\_ Петренко В.И.

«\_\_\_»\_\_\_\_\_\_\_\_\_\_ 2020 г.

СОГЛАСОВАНО

Начальник УДОПК СКФУ

\_\_\_\_\_\_\_\_\_\_\_\_\_ Федотова Н.Н.

«\_\_\_»\_\_\_\_\_\_\_\_\_\_ 2020 г.

Ставрополь, 2020 г

**Общее описание программы**

1. **Цель реализации программы**

Целью реализации программы является комплексное обновление знаний по информационным и цифровым технологиям, необходимым в профессиональной деятельности, прочное усвоение слушателями фундаментальных основ и принципов общей стратегии кибербезопасности, в рамках которой необходимо использовать структурный подход к менеджменту инцидентов, практики применения данных технологий, а также совершенствование умений и навыков слушателей с учетом специализации их профессиональной деятельности, повышения профессионального уровня в рамках имеющейся квалификации.

«Менеджмент инцидентов кибербезопасности» – практико-ориентированная дополнительная профессиональная программа повышения квалификации, нацелена на формирование практических умений, навыков и (или) приобретение опыта, необходимого для выполнения вида профессиональной деятельности №06.032 «Защита информации в компьютерных системах и сетях», конкретного самостоятельного вида деятельности при соответствии требованиям работодателя, либо осуществление работы по укрупненной группе специальностей «Информационная безопасность» наряду с основным видом деятельности в области цифровой экономики и соответствует области «Кибербезопасность и защита данных».

Программа соответствует действующему законодательству РФ (Федеральному закону «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ (актуальная редакция), Приказу Министерства образования и науки Российской Федерации (Минобрнауки России) от 1 июля 2013 г. № 499 г. Москва «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам», Приказом Министерства образования и науки РФ от 23 августа 2017 г. № 816 «Об утверждении Порядка применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ»).

Программа соответствует профессиональному стандарту №842 «Специалист по безопасности компьютерных систем и сетей».

1. **Планируемые результаты обучения**

Знать методы определения и построения моделей угроз информационной безопасности объектов информатизации; существующие подходы и методы построения моделей нарушителей информационной безопасности; порядок и методы организации и осуществления работ и мероприятий по обеспечению информационной безопасности объектов информатизации на базе защищенном исполнении; способы и методы анализа систем обеспечения информационной безопасности объектов информатизации;

Уметь проводить обследование объектов информатизации на базе компьютерных систем в защищенном исполнении; разрабатывать модели угроз и нарушителей информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении; формировать требования к обеспечению информационной безопасности и перечень функций безопасности; выбирать рациональные способы и средства реализации функций безопасности объекта информатизации на базе компьютерных систем в защищенном исполнении; проводить анализ проектных решений на предмет их соответствия требованиям по обеспечению информационной безопасности; организовать работы по реализации процессов проектирования, создания, эксплуатации объектов информатизации на базе компьютерных систем в защищенном исполнении, обеспечивать информационную безопасность этих процессов; - разрабатывать проекты документов по обеспечению информационной безопасности объектов информатизации.

Владеть навыками организации и проведения обследования объектов информатизации и условий их размещения; навыками и средствами проектирования систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении.

1. **Категория слушателей:**

Лица со средним профессиональным и/или высшим образованием, не получающие пенсионные выплаты.

Требований к квалификации нет.

Требований к наличию опыта профессиональной деятельности нет.

Базовые знания в области информатики и информационных технологий

1. **Учебный план программы Менеджмент инцидентов кибербезопасности**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№**  **п/п** | **Наименование модулей, тем** | **Всего**  **часов** | **В том числе** | | | **Форма проведения занятий** |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Входное анкетирование, тестирование, диагностика | 4 | 0 | 4 | 0 | Компьютерное тестирование |
| 2 | Разработка и документирование политики менеджмента инцидентов кибербезопасности | 10 | 4 | 4 | 2 | Вебинар |
| 3 | Формы, процедуры и инструменты поддержки обнаружения, оповещения, оценки и реагирования на инциденты кибербезопасности | 10 | 4 | 4 | 2 | Вебинар |
| 4 | Обновление политик менеджмента информационной безопасности и рисков | 14 | 4 | 8 | 2 | Вебинар |
| 5 | Обнаружение и оповещение о возникновении событий кибербезопасности (человеком или автоматическими средствами) | 10 | 4 | 4 | 2 | Вебинар |
| 6 | Сбор информации, связанной с событиями кибербезопасности, оценка этой информации с целью отнесения к категории инцидентов кибербезопасности | 10 | 2 | 6 | 2 | Вебинар |
| 7 | Способы реагирования на инциденты кибербезопасности | 12 | 2 | 8 | 2 | Вебинар |
| 8 | Итоговая диагностика | 2 | 0 | 2 | 0 | Тестирование |
|  | **Всего** | **72** | **20** | **40** | **12** |  |

1. **Календарный план-график программы Менеджмент инцидентов кибербезопасности**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование учебных модулей** | **Трудоёмкость (час)** | **Сроки обучения** |
| 1 | Входное анкетирование, тестирование, диагностика | 4 | 02.11.2020 - 02.11.2020 |
| 2 | Разработка и документирование политики менеджмента инцидентов кибербезопасности | 10 | 02.11.2020 - 03.11.2020 |
| 3 | Формы, процедуры и инструменты поддержки обнаружения, оповещения, оценки и реагирования на инциденты кибербезопасности | 10 | 03.11.2020 -  04.11.2020 |
| 4 | Обновление политик менеджмента информационной безопасности и рисков | 14 | 05.11.2020 -  06.11.2020 |
| 5 | Обнаружение и оповещение о возникновении событий кибербезопасности (человеком или автоматическими средствами) | 10 | 09.11.2020 -  10.11.2020 |
| 6 | Сбор информации, связанной с событиями кибербезопасности, оценка этой информации с целью отнесения к категории инцидентов кибербезопасности | 10 | 11.11.2020-12.11.2020 |
| 7 | Способы реагирования на инциденты кибербезопасности | 12 | 12.11.2020-13.11.2020 |
| 8 | Итоговая диагностика | 2 | 13.11.2020 |
| **Всего:** | | 72 | 02.11.2020 - 13.11.2020 |

Максимальное количество человек, которые могут одновременно обучаться по образовательной программе в организации: 300

Минимальное количество человек, которые могут быть зачислены для обучения по образовательной программе: 1

1. **Учебный план программы Менеджмент инцидентов кибербезопасности**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№**  **п/п** | **Наименование модулей, тем** | **Всего**  **часов** | **В том числе** | | | **Форма проведения занятий** |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Входное анкетирование, тестирование, диагностика | 4 | 0 | 4 | 0 | Компьютерное тестирование |
| 2 | Разработка и документирование политики менеджмента инцидентов кибербезопасности | 10 | 4 | 4 | 2 | Вебинар, выполнение заданий |
| 3 | Формы, процедуры и инструменты поддержки обнаружения, оповещения, оценки и реагирования на инциденты кибербезопасности | 10 | 4 | 4 | 2 | Вебинар, выполнение заданий |
| 4 | Обновление политик менеджмента информационной безопасности и рисков | 14 | 4 | 8 | 2 | Вебинар, выполнение заданий |
| 5 | Обнаружение и оповещение о возникновении событий кибербезопасности (человеком или автоматическими средствами) | 10 | 4 | 4 | 2 | Вебинар, выполнение заданий |
| 6 | Сбор информации, связанной с событиями кибербезопасности, оценка этой информации с целью отнесения к категории инцидентов кибербезопасности | 10 | 2 | 6 | 2 | Вебинар, выполнение заданий |
| 7 | Способы реагирования на инциденты кибербезопасности | 12 | 2 | 8 | 2 | Вебинар, выполнение заданий |
| 8 | Итоговая диагностика | 2 | 0 | 2 | 0 | Тестирование |
|  | **Всего** | **72** | **20** | **40** | **12** |  |

1. **Учебная (рабочая) программа повышения квалификации Менеджмент инцидентов кибербезопасности**

Модуль 1 – разработка и документирование политики менеджмента инцидентов кибербезопасности.

Модуль 2 – формы, процедуры и инструменты поддержки обнаружения, оповещения, оценки и реагирования на инциденты кибербезопасности.

Модуль 3 – обновление политик менеджмента информационной безопасности и рисков на всех уровнях, то есть на корпоративном и для каждой системы, сервиса и сети отдельно с учетом системы менеджмента инцидентов кибербезопасности.

Модуль 4 – обнаружение и оповещение о возникновении событий кибербезопасности (человеком или автоматическими средствами).

Модуль 5 – сбор информации, связанной с событиями кибербезопасности, оценка этой информации с целью отнесения к категории инцидентов кибербезопасности.

Модуль 6 – способы реагирования на инциденты кибербезопасности.

**Описание практико-ориентированных заданий и кейсов**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Номер темы/модуля** | **Наименование практического занятия** | **Описание** |
| **1** | **1** | Разработка и документирование политики менеджмента инцидентов кибербезопасности | Изучение основных регламентирующих документов о политике менеджмента инцидентов ИБ |
| **2** | **2** | Формы, процедуры и инструменты поддержки обнаружения, оповещения, оценки и реагирования на инциденты кибербезопасности | Изучение основных форм, процедур и инструментов поддержки обнаружения, оповещения, оценки и реагирования на инциденты кибербезопасности |
| **3** | **3** | Обновление политик менеджмента информационной безопасности и рисков | Изучение правил обновления политик менеджмента информационной безопасности и рисков |
| **4** | **4** | Обнаружение и оповещение о возникновении событий кибербезопасности (человеком или автоматическими средствами) | Изучение правил, методов и технологий обнаружения и оповещения о возникновении событий кибербезопасности (человеком или автоматическими средствами) |
| **5** | **5** | Сбор информации, связанной с событиями кибербезопасности, оценка этой информации с целью отнесения к категории инцидентов кибербезопасности | Изучение технологий сбора информации, связанной с событиями кибербезопасности, оценка этой информации с целью отнесения к категории инцидентов кибербезопасности |
| **6** | **6** | Способы реагирования на инциденты кибербезопасности | Изучение правил, методов, способов и технологий реагирования на инциденты кибербезопасности |

**8.Оценочные материалы по образовательной программе**

**8.1. Вопросы тестирования по модулям**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ модуля** | **Вопросы входного тестирования** | **Вопросы промежуточного тестирования** | **Вопросы итогового тестирования** |
| **1** | Кто является основным ответственным за определение уровня классификации информации?  -: Руководитель среднего звена  -: Высшее руководство  +: Владелец  -: Пользователь | Кто является основным ответственным за определение уровня классификации информации?  -: Руководитель среднего звена  -: Высшее руководство  +: Владелец  -: Пользователь | Кто является основным ответственным за определение уровня классификации информации?  -: Руководитель среднего звена  -: Высшее руководство  +: Владелец  -: Пользователь |
| **1** | S: Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?  +: Сотрудники  -: Хакеры  -: Атакующие  -: Контрагенты (лица, работающие по договору) | S: Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?  +: Сотрудники  -: Хакеры  -: Атакующие  -: Контрагенты (лица, работающие по договору) | S: Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?  +: Сотрудники  -: Хакеры  -: Атакующие  -: Контрагенты (лица, работающие по договору) |
| **1** | S: Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?  -: Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования  -: Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации  +: Улучшить контроль за безопасностью этой информации  -: Снизить уровень классификации этой информации | S: Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?  -: Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования  -: Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации  +: Улучшить контроль за безопасностью этой информации  -: Снизить уровень классификации этой информации | S: Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?  -: Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования  -: Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации  +: Улучшить контроль за безопасностью этой информации  -: Снизить уровень классификации этой информации |
| **1** | S: Что такое процедура?  -: Правила использования программного и аппаратного обеспечения в компании  +: Пошаговая инструкция по выполнению задачи  -: Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах  -: Обязательные действия | S: Что такое процедура?  -: Правила использования программного и аппаратного обеспечения в компании  +: Пошаговая инструкция по выполнению задачи  -: Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах  -: Обязательные действия | S: Что такое процедура?  -: Правила использования программного и аппаратного обеспечения в компании  +: Пошаговая инструкция по выполнению задачи  -: Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах  -: Обязательные действия |
| **2** | S: Методические документы определяют  +: Основные процессы и этапы работ по разработке политик менеджмента инцидентов кибербезопасности  -: Набор правил  -: Систему разработки ИС  -: Технологию проектирования ИС | S: Методические документы определяют  +: Основные процессы и этапы работ по разработке политик менеджмента инцидентов кибербезопасности  -: Набор правил  -: Систему разработки ИС  -: Технологию проектирования ИС | S: Методические документы определяют  +: Основные процессы и этапы работ по разработке политик менеджмента инцидентов кибербезопасности  -: Набор правил  -: Систему разработки ИС  -: Технологию проектирования ИС |
| **2** | S: Внешние угрозы от киберпреступников могут использовать ### в сетевых устройствах или социальную инженерию, например обман, чтобы получить доступ.  +: Уязвимости  S: Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?  -: Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски  -: Когда риски не могут быть приняты во внимание по политическим соображениям  -: Когда необходимые защитные меры слишком сложны  +: Когда стоимость контрмер превышает ценность актива и потенциальные потери | S: Внешние угрозы от киберпреступников могут использовать ### в сетевых устройствах или социальную инженерию, например обман, чтобы получить доступ.  +: Уязвимости  S: Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?  -: Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски  -: Когда риски не могут быть приняты во внимание по политическим соображениям  -: Когда необходимые защитные меры слишком сложны  +: Когда стоимость контрмер превышает ценность актива и потенциальные потери | S: Внешние угрозы от киберпреступников могут использовать ### в сетевых устройствах или социальную инженерию, например обман, чтобы получить доступ.  +: Уязвимости  S: Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?  -: Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски  -: Когда риски не могут быть приняты во внимание по политическим соображениям  -: Когда необходимые защитные меры слишком сложны  +: Когда стоимость контрмер превышает ценность актива и потенциальные потери |
| **2** | S: Что такое политики безопасности?  -: Пошаговые инструкции по выполнению задач безопасности  -: Общие руководящие требования по достижению определенного уровня безопасности  +: Широкие, высокоуровневые заявления руководства  -: Детализированные документы по обработке инцидентов безопасности | S: Что такое политики безопасности?  -: Пошаговые инструкции по выполнению задач безопасности  -: Общие руководящие требования по достижению определенного уровня безопасности  +: Широкие, высокоуровневые заявления руководства  -: Детализированные документы по обработке инцидентов безопасности | S: Что такое политики безопасности?  -: Пошаговые инструкции по выполнению задач безопасности  -: Общие руководящие требования по достижению определенного уровня безопасности  +: Широкие, высокоуровневые заявления руководства  -: Детализированные документы по обработке инцидентов безопасности |
| **2** | S: Какая из приведенных техник является самой важной при выборе конкретных защитных мер?  -: Анализ рисков  +: Анализ затрат / выгоды  -: Результаты ALE  -: Выявление уязвимостей и угроз, являющихся причиной риска | S: Какая из приведенных техник является самой важной при выборе конкретных защитных мер?  -: Анализ рисков  +: Анализ затрат / выгоды  -: Результаты ALE  -: Выявление уязвимостей и угроз, являющихся причиной риска | S: Какая из приведенных техник является самой важной при выборе конкретных защитных мер?  -: Анализ рисков  +: Анализ затрат / выгоды  -: Результаты ALE  -: Выявление уязвимостей и угроз, являющихся причиной риска |
| **3** | S: Тактическое планирование – это:  +: Среднесрочное планирование  -: Долгосрочное планирование  -: Ежедневное планирование  -: Планирование на 6 месяцев | S: Тактическое планирование – это:  +: Среднесрочное планирование  -: Долгосрочное планирование  -: Ежедневное планирование  -: Планирование на 6 месяцев | S: Тактическое планирование – это:  +: Среднесрочное планирование  -: Долгосрочное планирование  -: Ежедневное планирование  -: Планирование на 6 месяцев |
| **3** | S: Эффективная программа безопасности требует сбалансированного применения:  +: Технических и нетехнических методов  -: Контрмер и защитных механизмов  -: Физической безопасности и технических средств защиты  -: Процедур безопасности и шифрования | S: Эффективная программа безопасности требует сбалансированного применения:  +: Технических и нетехнических методов  -: Контрмер и защитных механизмов  -: Физической безопасности и технических средств защиты  -: Процедур безопасности и шифрования | S: Эффективная программа безопасности требует сбалансированного применения:  +: Технических и нетехнических методов  -: Контрмер и защитных механизмов  -: Физической безопасности и технических средств защиты  -: Процедур безопасности и шифрования |
| **3** | S: Что из перечисленного не является целью проведения анализа рисков?:  +: Делегирование полномочий  -: Количественная оценка воздействия потенциальных угроз  -: Выявление рисков  -: Определение баланса между воздействием риска и стоимостью необходимых контрмер | S: Что из перечисленного не является целью проведения анализа рисков?:  +: Делегирование полномочий  -: Количественная оценка воздействия потенциальных угроз  -: Выявление рисков  -: Определение баланса между воздействием риска и стоимостью необходимых контрмер | S: Что из перечисленного не является целью проведения анализа рисков?:  +: Делегирование полномочий  -: Количественная оценка воздействия потенциальных угроз  -: Выявление рисков  -: Определение баланса между воздействием риска и стоимостью необходимых контрмер |
| **3** | S: Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?  -: Поддержка  +: Выполнение анализа рисков  -: Определение цели и границ  -: Делегирование полномочий | S: Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?  -: Поддержка  +: Выполнение анализа рисков  -: Определение цели и границ  -: Делегирование полномочий | S: Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?  -: Поддержка  +: Выполнение анализа рисков  -: Определение цели и границ  -: Делегирование полномочий |
| **3** | S: Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?  -: Чтобы убедиться, что проводится справедливая оценка  -: Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ  +: Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа  -: Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку | S: Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?  -: Чтобы убедиться, что проводится справедливая оценка  -: Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ  +: Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа  -: Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку | S: Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?  -: Чтобы убедиться, что проводится справедливая оценка  -: Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ  +: Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа  -: Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку |
| **4** | S: Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?  -: Анализ связующего дерева  -: AS/NZS  -: NIST  +: Анализ сбоев и дефектов | S: Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?  -: Анализ связующего дерева  -: AS/NZS  -: NIST  +: Анализ сбоев и дефектов | S: Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?  -: Анализ связующего дерева  -: AS/NZS  -: NIST  +: Анализ сбоев и дефектов |
| **4** | S: Защита информации от утечки – это деятельность по предотвращению:  -: Получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации  -: Воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации  -: Воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений  +: Неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа  -: Несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации | S: Защита информации от утечки – это деятельность по предотвращению:  -: Получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации  -: Воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации  -: Воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений  +: Неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа  -: Несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации | S: Защита информации от утечки – это деятельность по предотвращению:  -: Получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации  -: Воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации  -: Воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений  +: Неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа  -: Несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации |
| **4** | S: К посторонним лицам нарушителям информационной безопасности относится:  -: Представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации  -: Персонал, обслуживающий технические средства  -: Технический персонал, обслуживающий здание  -: Пользователи  -: Сотрудники службы безопасности  +: Представители конкурирующих организаций  -: Лица, нарушившие пропускной режим | S: К посторонним лицам нарушителям информационной безопасности относится:  -: Представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации  -: Персонал, обслуживающий технические средства  -: Технический персонал, обслуживающий здание  -: Пользователи  -: Сотрудники службы безопасности  +: Представители конкурирующих организаций  -: Лица, нарушившие пропускной режим | S: К посторонним лицам нарушителям информационной безопасности относится:  -: Представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации  -: Персонал, обслуживающий технические средства  -: Технический персонал, обслуживающий здание  -: Пользователи  -: Сотрудники службы безопасности  +: Представители конкурирующих организаций  -: Лица, нарушившие пропускной режим |
| **5** | S: К внутренним нарушителям информационной безопасности относится:  -: Клиенты  -: Пользователи системы  -: Посетители  -: Любые лица, находящиеся внутри контролируемой территории  -: Представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации  -: Персонал, обслуживающий технические средства  -: Сотрудники отделов разработки и сопровождения ПО  +: Технический персонал, обслуживающий здание | S: К внутренним нарушителям информационной безопасности относится:  -: Клиенты  -: Пользователи системы  -: Посетители  -: Любые лица, находящиеся внутри контролируемой территории  -: Представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации  -: Персонал, обслуживающий технические средства  -: Сотрудники отделов разработки и сопровождения ПО  +: Технический персонал, обслуживающий здание | S: К внутренним нарушителям информационной безопасности относится:  -: Клиенты  -: Пользователи системы  -: Посетители  -: Любые лица, находящиеся внутри контролируемой территории  -: Представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации  -: Персонал, обслуживающий технические средства  -: Сотрудники отделов разработки и сопровождения ПО  +: Технический персонал, обслуживающий здание |
| **5** | S: Активный перехват информации – это перехват, который:  -: заключается в установке подслушивающего устройства в аппаратуру средств обработки информации  -: основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций  -: неправомерно использует технологические отходы информационного процесса  -: осуществляется путем использования оптической техники  +: осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера | S: Активный перехват информации – это перехват, который:  -: заключается в установке подслушивающего устройства в аппаратуру средств обработки информации  -: основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций  -: неправомерно использует технологические отходы информационного процесса  -: осуществляется путем использования оптической техники  +: осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера | S: Активный перехват информации – это перехват, который:  -: заключается в установке подслушивающего устройства в аппаратуру средств обработки информации  -: основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций  -: неправомерно использует технологические отходы информационного процесса  -: осуществляется путем использования оптической техники  +: осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера |

**8.2. Критерии и шкала оценки**

Промежуточная аттестация

Учебным планом предусмотрен зачет по результатам тестирования.

Рейтинговый балл, выставляемый за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

|  |  |
| --- | --- |
| Уровень выполнения контрольного задания | Рейтинговый балл (в % от максимального балла за контрольное задание) |
| Отличный | 100 |
| Хороший | 80 |
| Удовлетворительный | 60 |
| Неудовлетворительный | 0 |

**8.3. Примеры контрольных заданий по модулям или всей образовательной программе**

**Практическое занятие № 1. Разработка и документирование политики менеджмента инцидентов кибербезопасности**

**Цель**: изучить основные угрозы информации в компьютерных системах.

## Ход работы:

1. По согласованию с преподавателем определить исходные данные:
   * Вид предприятия, краткое описание структуры предприятия, видов продукции и процессов.
   * Краткое описание инфраструктуры и ресурсов.
   * Описание информационной инфраструктуры предприятия.
2. Определить основные виды объектов защиты для данного предприятия. Для каждого вида объектов привести конкретные примеры. Объекты защиты выбирать в составе оборудования, инфраструктуры, персонала предприятия.
3. Определить основные виды угроз и способов их реализации для основных объектов защиты для заданного предприятия.
4. Для каждого вида угроз определить основные способы и средства предотвращения угроз.
5. Сформулировать основные элементы системы инженерно-технической защиты информации для заданного предприятия.

Рекомендуется изложить информацию в табличной форме, например:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №п/п | Элемент орг- структуры или  инфраструктуры | Вид угрозы | Методы защиты | Средства инженерно- технической защиты |
| 1 | 2 | 3 | 4 | 5 |

**8.4.** **Тесты и обучающие задачи (кейсы), иные практикоориентированные формы заданий**

**Пример тестового задания по практической работе:**

**Что понимается под инцидентом ИБ и процессом реагирования на инцидент?**

Инцидентом информационной безопасности называется любое незаконное, неразрешенное (в том числе политикой ИБ) или неприемлемое действие, которое совершается в информационной системе. Организация процесса реагирования на инцидент преследует такие цели.

* Предупредить нескоординированные действия и в кратчайшие сроки восстановить работоспособность компании при возникновении инцидента.
* Подтвердить или опровергнуть факт инцидента ИБ.
* Представить детализированный отчет о произошедшем инциденте и полезные рекомендации. Создать условия для накопления и хранения точной информации о компьютерных инцидентах. Обеспечить быстрое обнаружение и/или предупреждение подобных инцидентов в будущем (путем анализа "прошедших уроков", изменения политики ИБ, модернизации системы ИБ и др.).
* Обеспечить сохранность и целостность доказательств произошедшего инцидента. Создать условия для возбуждения гражданского или уголовного дела против злоумышленника(-ов). Защитить частные права, установленные законом.
* Минимизировать нарушение порядка работы и повреждения данных ИТ-системы. Минимизировать последствия нарушения конфиденциальности, целостности и доступности ИТ-системы.
* Защитить репутацию компании и ее ресурсы.
* Провести обучение сотрудников компании о процессе реагирования на инцидент.

**8.5. Описание процедуры оценивания результатов обучения**

Оценка «отлично» выставляется, если студент:

знает полностью: направления развития информационных (телекоммуникационных) технологий, способы и механизмы прогнозирования эффективности функционирования, оценки затрат и рисков, формирования политики безопасности объектов защиты; методики разработки систем, комплексов, средств и технологий обеспечения информационной безопасности;

умеет полностью: анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты; разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;

владеет полностью: способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты; способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности.

Оценка «хорошо» выставляется, если студент:

знает на хорошем уровне: направления развития информационных (телекоммуникационных) технологий, способы и механизмы прогнозирования эффективности функционирования, оценки затрат и рисков, формирования политики безопасности объектов защиты; методики разработки систем, комплексов, средств и технологий обеспечения информационной безопасности;

умеет на хорошем уровне: анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты; разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;

владеет на хорошем уровне: способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты; способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности.

Оценка «удовлетворительно» выставляется, если студент:

знает частично: направления развития информационных (телекоммуникационных) технологий, способы и механизмы прогнозирования эффективности функционирования, оценки затрат и рисков, формирования политики безопасности объектов защиты; методики разработки систем, комплексов, средств и технологий обеспечения информационной безопасности;

умеет частично: анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты; разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;

владеет частично: способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты; способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности.

Оценка «неудовлетворительно» выставляется, если студент:

знает на недостаточном уровне: направления развития информационных (телекоммуникационных) технологий, способы и механизмы прогнозирования эффективности функционирования, оценки затрат и рисков, формирования политики безопасности объектов защиты; методики разработки систем, комплексов, средств и технологий обеспечения информационной безопасности;

умеет на недостаточном уровне: анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты; разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности;

владеет на недостаточном уровне: способностью анализировать направления развития информационных (телекоммуникационных) технологий, прогнозировать эффективность функционирования, оценивать затраты и риски, формировать политику безопасности объектов защиты; способностью разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности.

**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** | **Огур Максим Геннадьевич** | Старший преподаватель кафедры прикладной математики и компьютерной безопасности института математики и информационных технологий имени профессора Н.И. Червякова Северо-Кавказского федерального университета | [**https://www.ncfu.ru/for-employee/list-of-employees/employee/12e34695-53b2-11ea-821d-0050568c7ce8/**](https://www.ncfu.ru/for-employee/list-of-employees/employee/12e34695-53b2-11ea-821d-0050568c7ce8/) |  | **Согласен** |
| **2** | **Березницкий Андрей Сергеевич** | Доцент, к.э.н., доцент кафедры прикладной математики и компьютерной безопасности института математики и информационных технологий имени профессора Н.И. Червякова Северо-Кавказского федерального университета,  заместитель начальника Центра -зав. отделом по производству экспертиз и экспертных исследований по делам, связанным с проявлением экстремизма ФБУ Северо-Кавказского РЦСЭ Минюста России |  |  | **Согласен** |

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

|  |  |
| --- | --- |
| **Учебно-методические материалы** | |
| Методы, формы и технологии | Методические разработки,  материалы курса, учебная литература |
| Лекционные занятия. В виде изучения курса лекций | Курс лекции к программе |
| Практические занятия. Изучение методических рекомендаций по выполнению практических занятий. Выполнение индивидуальных заданий. Изучение дополнительной литературы | Методические указания к выполнению практических занятий.  Варианты индивидуальных заданий |
| Самостоятельная работа. Выполнение индивидуальных заданий для закрепления знаний | Методические указания к выполнению практических занятий.  Варианты индивидуальных заданий |
| Изучение дополнительной литературы | Основная |
| Проведение индивидуальных и групповых консультаций по практическим работам в режиме видеоконференцсвязи |  |
| 1. Нестеров, С.А. Основы информационной безопасности. [Электронный ресурс]: учеб. пособие. Электрон. дан. СПб.: Лань, 2017. 324 с. Режим доступа: http://e.lanbook.com/book/90153  2. Безопасность и управление доступом в информационных системах: Учебное пособие / А.В. Васильков, И.А.Васильков. – М.: Форум: НИЦ ИНФРА-М, 2013. - 368 с.: ил.; 60x90 1/16. – Профессиональное образование) (переплет) ISBN 978-5-91134-360-6 - http://znanium.com/bookread2.php?book=405313  3. Жукова, М. Н. Управление информационной безопасностью. Ч. 2. Управление инцидентами информационной безопасности [Электронный ресурс]: учеб.пособие / М. Н. Жукова, В. Г. Жуков, В. В. Золотарев. – Красноярск:Сиб. гос. аэрокосмич. ун-т, 2012. – http://znanium.com/bookread2.php?book=463061 | |
| 1.Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416 с.: ил.; 60x90 1/16. – (Профессиональное образование). (переплет) ISBN 978-5-8199-0331-5 - http://znanium.com/bookread2.php?book=423927  2.Информационная безопасность конструкций ЭВМ и систем: учебное пособие / Е.В. Глинская, Н.В. Чичварин. – М.: НИЦ ИНФРА-М, 2016. - 118 с. URL: http://znanium.com/bookread2.php?book=507334  3. Партыка Т. Л. Информационная безопасность [Электронный ресурс]: Учебное пособие /Т.Л. Партыка, И.И. Попов. – 5-e изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. – 432 с.: ил.; 60x90 1/16. – (Профессиональное образование). ISBN 978-5-91134-627-0, 1000 экз. http://znanium.com/bookread2.php?book=420047 | |

|  |  |
| --- | --- |
| **Информационное сопровождение** | |
| Электронные  образовательные ресурсы | Электронные  информационные ресурсы |
| Образовательный портал Северо-Кавказского федерального университета  https://el.ncfu.ru/ | https://rvision.pro/blog-posts/upravlenie-intsidentami-informatsionnoj-bezopasnosti/ |
|  | http://docs.cntd.ru/document/1200068822 |

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

|  |  |
| --- | --- |
| Вид занятий | Наименование оборудования,  программного обеспечения |
| Лекции | Для слушателей - ноутбук с возможностью подключения к сети Интернет.  Со стороны университета занятия проводятся в лаборатории расследования компьютерных преступлений и инцидентов кафедры прикладной математики и компьютерной безопасности института математики и информационных технологий имени профессора Н.И. Червякова Северо-Кавказского федерального университета. |
| Практические занятия | Для слушателей - ноутбук с возможностью подключения к сети Интернет.  Со стороны университета занятия проводятся в лаборатории расследования компьютерных преступлений и инцидентов кафедры прикладной математики и компьютерной безопасности института математики и информационных технологий имени профессора Н.И. Червякова Северо-Кавказского федерального университета. |
| Самостоятельная работа | Для слушателей - ноутбук с возможностью подключения к сети Интернет.  Со стороны университета занятия проводятся в лаборатории расследования компьютерных преступлений и инцидентов кафедры прикладной математики и компьютерной безопасности института математики и информационных технологий имени профессора Н.И. Червякова Северо-Кавказского федерального университета. |

**Объем образовательной программы:** 72 ч**.** (акад.час 45 минут)

**Форма обучения:** Электронная реализация с применением дистанционных образовательных технологий, с возможностью передачи данных в форме элементов цифрового следа

**Уровень сложности содержания образовательной программы:**

Программа может соответствовать двум уровням сложности – базовому и продвинутому уровням.

**Режим занятий:** ежедневно, 6-12 часов в день.

**Стоимость обучения:** 30 тыс. руб.

Возможные сценарии профессиональной траектории слушателей **(**по итогам освоения образовательной программы): Трудоустройство, Развитие компетенций в текущей сфере занятости, Переход в новую сферу занятости.

**Требования к уровню образования и (или) квалификации обучающегося:**

Необходимо наличие среднего профессионального или высшего образования по группам направлений и специальностей из списка:

* 02.00.00 – Компьютерные и информационные науки;
* 09.00.00 – Информатика и вычислительная техника;
* 10.00.00 – Информационная безопасность.

**Ссылка на действующую интернет-страницу образовательной программы:**

[**https://el.ncfu.ru/course/view.php?id=1412**](https://el.ncfu.ru/course/view.php?id=1412)

[**https://www.ncfu.ru/education/dop-prof/proekt-cifrovoi-sertifikat/Menedjment-incidentov-kiberbezopasnosti/#**](https://www.ncfu.ru/education/dop-prof/proekt-cifrovoi-sertifikat/Menedjment-incidentov-kiberbezopasnosti/#)

[**https://www.ncfu.ru/education/dop-prof/proekt-cifrovoi-sertifikat/**](https://www.ncfu.ru/education/dop-prof/proekt-cifrovoi-sertifikat/)

**Ссылки на 3 (три) аналогичные образовательные программы иных организаций, осуществляющих обучение:**

[**https://itsecurity.ru/catalog/bt41/**](https://itsecurity.ru/catalog/bt41/)

(24 ак. часа, стоимость 32500 руб)

[**https://www.academyit.ru/courses/%D0%98%D0%91040/**](https://www.academyit.ru/courses/%D0%98%D0%91040/)

(40 часов, стоимость 57900 руб)

[**https://www.group-ib.ru/landing/incident-response-workshop.html?utm\_source=banner&utm\_medium=banner&utm\_campaign=ir**](https://www.group-ib.ru/landing/incident-response-workshop.html?utm_source=banner&utm_medium=banner&utm_campaign=ir)

(12 часов, стоимость 36000 руб)

**Учебно-методические материалы**

Примеры практико-ориентированных заданий и кейсов:

1. Задание основано на использовании Блока формирования изображений AccessData FTK.
2. Исправление взломанной конфигурации Linux-системы.
3. Студенты создадут свою собственную виртуальную среду с помощью VirtualBox и Ubuntu Linux. В получающейся сети студент настроит одну из систем Linux как брандмауэр и создаст политику обеспечения доступа, как потребуется в каждом из вопросов.
4. Введение в инструменты и приемы двоичного микропрограммного анализа. Объект - ведомая лаборатория исследования, которая представляет инструменты как binwalk, файл и dd и как они могут помочь в анализе двоичных блоков микропрограммы устройств.
5. Полиция расследует ряд похищений. Чучела животных похищаются из домов и продаются на международном нелегальном рынке.

Следователь совершил рейд на офис подозреваемого главаря. Команда Реагирования на инциденты смогла выполнить сбор данных на найденных устройствах и компьютерах. Подозреваемый утверждает, что он невиновен и что любое найденное доказательство было подброшено на его компьютер. Полиция также получила ноутбук от одного из предполагаемых покупателей чучела животного. Задание состоит в том, чтобы проанализировать полученные данные и ответить на вопросы в приложенном документе так, чтобы следователь мог арестовать причастных к преступлениям.

1. Студентам будет рассказано об использовании Wireshark для просмотра файлов, переданных через HTTP. Студентов научат, как настроить автоматический и ручной карвинг файлов. Далее, заданием для студентов станет настройка карвинга по протоколу FTP.

*Формы и технологии, применяемые при реализации программы*:

Программа реализуется с применением дистанционных образовательных технологий (ДОТ) на базе системы управления обучением СКФУ LMS Moodle, образовательного портала «Электронный Кампус СКФУ» https://ecampus.ncfii.ru (далее - еКампус), платформ Cisco WebEx, BigBlueButton, обеспечивающих поддержку контактного взаимодействия преподавателя и обучающихся в дистанционном формате.

Видом проведения итоговой аттестации (контрольное мероприятие) с применением электронного обучения, дистанционных образовательных технологий является компьютерное тестирование.

Компьютерное тестирование проводится с использованием специализированного программного обеспечения посредством сервисов системы управления обучением LMS Moodle.

### ПАСПОРТ КОМПЕТЕНЦИИ

**Дополнительная профессиональная программа**

**повышения квалификации**

**«Менеджмент инцидентов кибербезопасности»**

**Федеральное государственное автономное образовательное учреждение высшего образования**

**«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | **Наименование компетенции** | | Способность использовать современные технологии поиска, фиксации, анализа и документирования следов компьютерных преступлений, правонарушений и инцидентов | |
| 2. | **Указание типа компетенции** | Общекультурная универсальная |  | |
| Общепрофессиональная |  | |
| Профессиональная |  | |
| Профессионально-специализированная | + | |
| 3 | **Определение, содержание и основные сущностные характеристики компетенции** | | Получение навыков разработки и модернизации политик кибербезопасности, получения навыка реагирования на инциденты кибербезопасности | |
| 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.) | Знать методы определения и построения моделей угроз информационной безопасности объектов информатизации; существующие подходы и методы построения моделей нарушителей информационной безопасности;  Уметь проводить обследование объектов информатизации на базе компьютерных систем в защищенном исполнении; разрабатывать модели угроз и нарушителей информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении.  Владеть навыками организации и проведения обследования объектов информатизации и условий их размещения; - навыками и средствами проектирования |
|  |  | | **Базовый уровень**  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, сложности.) | Знать методы определения и построения моделей угроз информационной безопасности объектов информатизации; - существующие подходы и методы построения моделей нарушителей информационной безопасности; - порядок и методы организации и осуществления работ и мероприятий по обеспечению информационной безопасности объектов информатизации на базе защищенном исполнении.  Уметь проводить обследование объектов информатизации на базе компьютерных систем в защищенном исполнении; разрабатывать модели угроз и нарушителей информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении; формировать требования к обеспечению информационной безопасности и перечень функций безопасности; - выбирать рациональные способы и средства реализации функций безопасности объекта информатизации на базе компьютерных систем в защищенном исполнении.  Владеть навыками организации и проведения обследования объектов информатизации и условий их размещения; навыками и средствами проектирования |
| 3. |  | | **Продвинутый**  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности) | Знать методы определения и построения моделей угроз информационной безопасности объектов информатизации; существующие подходы и методы построения моделей нарушителей информационной безопасности; порядок и методы организации и осуществления работ и мероприятий по обеспечению информационной безопасности объектов информатизации на базе защищенном исполнении; способы и методы анализа систем обеспечения информационной безопасности объектов информатизации.  Уметь проводить обследование объектов информатизации на базе компьютерных систем в защищенном исполнении; разрабатывать модели угроз и нарушителей информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении; формировать требования к обеспечению информационной безопасности и перечень функций безопасности; - выбирать рациональные способы и средства реализации функций безопасности объекта информатизации на базе компьютерных систем в защищенном исполнении; проводить анализ проектных решений на предмет их соответствия требованиям по обеспечению информационной безопасности.  Владеть навыками организации и проведения обследования объектов информатизации и условий их размещения; - навыками и средствами проектирования. |
|  |  | | **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 ситуация повышенной сложности.) | Знать методы определения и построения моделей угроз информационной безопасности объектов информатизации; существующие подходы и методы построения моделей нарушителей информационной безопасности; - порядок и методы организации и осуществления работ и мероприятий по обеспечению информационной безопасности объектов информатизации на базе защищенном исполнении; способы и методы анализа систем обеспечения информационной безопасности объектов информатизации.  Уметь проводить обследование объектов информатизации на базе компьютерных систем в защищенном исполнении; разрабатывать модели угроз и нарушителей информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении; формировать требования к обеспечению информационной безопасности и перечень функций безопасности; - выбирать рациональные способы и средства реализации функций безопасности объекта информатизации на базе компьютерных систем в защищенном исполнении; проводить анализ проектных решений на предмет их соответствия требованиям по обеспечению информационной безопасности; организовать работы по реализации процессов проектирования, создания, эксплуатации объектов информатизации на базе компьютерных систем в защищенном исполнении, обеспечивать информационную безопасность этих процессов; разрабатывать проекты документов по обеспечению информационной безопасности объектов информатизации.  Владеть навыками организации и проведения обследования объектов информатизации и условий их размещения; навыками и средствами проектирования |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | Компетенция связана со следующими компетенциями:  ОПК-8- способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач.  ОПК-9 - способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации. | |
| 6. | Средства и технологии оценки | | Тесты, кейс-тесты. | |

**VI.Иная информация о качестве и востребованности образовательной программы**

В очном формате программа была востребована для повышения квалификации сотрудников ГУ МВД России по Ставропольскому краю, а также для специалистов Северо-Кавказского регионального центра судебной экспертизы Министерства юстиции Российской Федерации.

**V.Рекомендации к программе от работодателей**:

Программа рекомендована к реализации компаниями ООО «ЕНДС-Ставрополь», Северо-Кавказским региональным центром судебной экспертизы Министерства юстиции Российской Федерации и ООО «Цитрикс».

Указанные организации готовы рассмотреть возможность трудоустройства слушателей, успешно прошедших обучение по данной образовательной программе.

Скан-копии писем прикреплены к пакету документов.

**VI.Указание на возможные сценарии профессиональной траектории граждан**

Трудоустройство, Развитие компетенций в текущей сфере занятости, Переход в новую сферу занятости в разрезе вида профессиональной деятельности №06.032 «Защита информации в компьютерных системах и сетях», конкретного самостоятельного вида деятельности при соответствии требованиям работодателя, либо осуществление работы по укрупненной группе специальностей «Информационная безопасность»

**VII.Дополнительная информация**

**VIII.Приложенные Скан-копии**

Полная скан копия утвержденной программы в формате PDF прикреплена к пакету документов.

И.о. проректора по учебной работе,

заместитель проректора Мезенцева О.С.