|  |  |
| --- | --- |
|  | Утверждаю:  Проректор по УР  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Т.А. Ольховая  «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_20\_\_ г. |

**Паспорт Образовательной программы**

**«Кибербезопасность и защита данных»**

|  |  |
| --- | --- |
| **Версия программы** | **1** |
| **Дата Версии** | **01.10.2020** |

1. **Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования  «Оренбургский государственный университет» |
| 1.2 | Логотип образовательной организации | **C:\Users\Podosenova\Desktop\Цифровая экономика\Документы для заявки\osu_sign.jpg** |
| 1.3 | Провайдер ИНН | **5612001360** |
| 1.4 | Ответственный за программу ФИО | **Влацкая Ирина Валерьевна** |
| 1.5 | Ответственный должность | заведующий кафедрой компьютерной безопасности и математического обеспечения информационных систем |
| 1.6 | Ответственный Телефон | **+79033603704** |
| 1.7 | Ответственный Е-mail | **irina.vlatskaya@yandex.ru** |

1. **Основные Данные**

|  |  |  |
| --- | --- | --- |
| **№** | **Название** | **Описание** |
| 2.1 | Название программы | **Кибербезопасность и защита данных** |
| 2.2 | Ссылка на страницу программы | [**http://www.osu.ru/doc/5024**](http://www.osu.ru/doc/5024) |
| 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 | **Имеется**  https://moodle.osu.ru/course/view.php?id=7648 |
| 2.4 | Уровень сложности | **Продвинутый** |
| 2.5 | Количество академических часов | **72 часа** |
|  | Практикоориентированный характер образовательной программы: не менее 50 % трудоёмкости учебной деятельности отведено практическим занятиям и (или) выполнению практических заданий в режиме самостоятельной работы | Практические занятия – 40 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 | **20 000 рублей**  https://www.ed.cibit.ru/programmy-obucheniya/persdannie/ 29 000 рублей  https://edu.softline.com/directions/bezopasnost-i-zashhita-dannyh/ 72 часа 39768 рублей/44187 рублей дист./очно  https://nousro.ru/pk-informatsionnaya-bezopasnost.php# 72 часа 20000 рублей/30000 рублей дист./очно |
| 2.7 | Минимальное количество человек на курсе | **15 человек** |
| 2.8 | Максимальное количество человек на курсе | **100** |
| 2.9 | Данные о количестве слушателей, ранее успешно прошедших обучение по образовательной программе | **0** (Но в ВУЗе уже несколько лет реализуется обучение по схожей программе: «Техническая защита информации ограниченного доступа, не содержащей сведения составляющие государственную тайну». Программа согласована с ФСТЭК РФ) |
| 2.10 | Формы аттестации | **зачет** |
|  | 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**

Реализация дополнительной образовательной программы «Кибербезопасность и защита данных» направлена на формирование и совершенствование профессиональных компетенций слушателей в области коммуникации в цифровой среде и безопасного использования программного обеспечения и данных. Данная программа позволит слушателям получить новые компетенции, необходимые специалистам, в том числе государственным гражданским служащим и муниципальным служащим для выполнения нового вида профессиональной деятельности «Кибербезопасность и защита данных».

Программа предназначена для слушателей, имеющих высшее образование по направлению подготовки (специальности) в области математических и естественных наук, инженерного дела, технологий и технологических наук в соответствии с перечнями специальностей и направлений подготовки высшего образования, утвержденными Министерством образования и науки Российской Федерации в соответствии с частью 8 статьи 11 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», подтвержденное документом об образовании.

**Цель программы**

Программа повышения квалификации «Кибербезопасность и защита данных» имеет своей целью формирование и совершенствование профессиональных компетенций слушателей в области коммуникации в цифровой среде и безопасного использования программного обеспечения и данных для решения своих профессиональных задач.

**Планируемые результаты обучения:**

5.1 Знание:

5.1.1 основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;

5.1.2 основные виды политик управления доступом и информационными потоками в компьютерных системах

5.2 Умение:

5.2.1 анализировать и оценивать угрозы информационной безопасности объекта;

5.2.2 применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях

5.3 Владеть:

5.3.1 навыками построения формальных моделей дискреционного, мандатного, ролевого управления доступом, моделей изолированной программной среды и безопасности информационных потоков

5.3.2 навыками настройки межсетевых экранов;

5.3.3 методиками анализа сетевого трафика.

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение  
высшего профессионального образования   
«Оренбургский государственный университет»

|  |  |
| --- | --- |
|  | Утверждаю:  Проректор по УР  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Т.А. Ольховая  «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_20\_\_ г. |

Дополнительная профессиональная программа повышения квалификации

«Кибербезопасность и защита данных»

72 часа

**ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ**

**1.Цель программы**

Программа повышения квалификации «Кибербезопасность и защита данных» имеет своей целью формирование и совершенствование профессиональных компетенций слушателей в области коммуникации в цифровой среде и безопасного использования программного обеспечения и данных для решения своих профессиональных задач.

**2.Планируемые результаты обучения:**

2.1. Знание (осведомленность в областях)

2.1.1 - знать нормативные правовые акты, методические документы, международные и национальные стандарты в области защиты информации;

2.1.2 - знать основы построения информационных систем и формирования информационных ресурсов;

2.1.3 - знать виды конфиденциальной информации;

2.1.4 - знать перечни сведений конфиденциального характера, основные требования и рекомендации по их защите;

2.2. Умение (способность к деятельности)

2.2.1. способность работать с действующей нормативной правовой и методической базой в области защиты информации;

2.1.2 способность применять программные средства системного, прикладного и специального назначения;

2.1.3 способность определять требования к программным и аппаратным средствам, предназначенным для хранения, обработки и передачи информации;

2.3. Навыки (использование конкретных инструментов)

2.3.1 навыки установки и настройки современных средств защиты информации, системного и прикладного программного обеспечения с учетом требований по безопасности информации;2

2.3.2 навыки работы в компьютерных сетях с учетом требований по безопасности информации.

2.3.2 навыки применения программно-аппаратных, криптографических и технических средств для защиты информации

**3. Категория слушателей**  Уровень образования лица, поступающего на обучение – высшее образование по направлению подготовки (специальности) в области математических и естественных наук, инженерного дела, технологий и технологических наук в соответствии с перечнями специальностей и направлений подготовки высшего образования, утвержденными Министерством образования и науки Российской Федерации в соответствии с частью 8 статьи 11 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации», подтвержденное документом об образовании.

**4.Учебный план программы «Кибербезопасность и защита данных»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль** | **Всего, час** | **Виды учебных занятий** | | |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| **1** | Модуль 1 | **16** | **8** | **6** | **2** |
| **2** | Модуль 2 | **14** | **4** | **6** | **4** |
| **3** | Модуль 3 | **42** | **10** | **24** | **8** |
| **Итоговая аттестация** | | **2** | **Зачёт** | | |

**5.Календарный план-график реализации образовательной программы** **«Кибербезопасность и защита данных»**

(01.11.2020 – 15.11.2020)

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование учебных модулей** | **Трудоёмкость (час)** | **Сроки обучения** |
| **1** | Модуль 1 Нормативно-правовая база обеспечения информационной безопасности | **16** | **01.11.2020 –**  **04.11.2020** |
| **2** | Модуль 2 Ответственность за нарушение требований в области информационной безопасности | **14** | **05.11.20 –**  **07.11.20 20** |
| **3** | Модуль 3 Порядок организации работ по защите информации | **42** | **08.11.2020 – 15.11.2020** |
| **Всего:** | | **72** | **01.11.2020 – 15.11.2020** |

**6.Учебно-тематический план программы «Кибербезопасность и защита данных»**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| №  п/п | ***Модуль/Тема*** | ***Виды учебных занятий.*** | | | | ***Формы контроля*** |
| ***Всего,***  ***час*** | **лекции** | **Практические**  **занятия** | **Самостоятельная работа** |
| **1** | **Нормативно-правовая база обеспечения информационной безопасности** | **16** | **8** | **6** | **2** | **Тестирование** |
| 1.1 | Доктрина информационной безопасности Российской Федерации | 2 | 2 | - |  |  |
| 1.2 | Государственная система защиты информации | 2 | 2 |  |  | - |
| 1.3 | Защита информации ограниченного доступа | 6 | 2 | 4 |  | - |
| 1.3 | Нормативные акты ФСТЭК и ФСБ России | 6 | 2 | 2 | 2 | - |
| **2** | **Ответственность за нарушение требований в области информационной безопасности** | **14** | **4** | **6** | **4** | **Тестирование** |
| 2.1 | Критерии отнесения информации к защищаемой. Понятие и виды ущерба от НСД. | 8 | 2 | 4 | 2 | - |
| 2.2 | Понятие и виды ущерба от НСД. Система современного законодательства, регламентирующая вопросы защиты информации и ответственности за нарушение информационной безопасности | 6 | 2 | 2 | 2 |  |
| **3.** | **Порядок организации работ по защите информации** | **42** | **10** | **24** | **8** | **Тестирование** |
| 3.1 | Система органов по технической защите информации в Российской Федерации | 4 | 2 | - | 2 | - |
| 3.2 | Технические каналы утечки информации | 4 |  | 4 |  | - |
| 3.3 | Средства выявления каналов утечки информации | 8 | 2 | 6 | 0 | - |
| 3.4 | Проблема НСД к информационным системам. Защита от физического доступа, электронные замки. Защита от НСД по компьютерным сетям | 4 | - | 2 | 2 | - |
| 3.5 | Модели разграничения доступа к компьютерным системам | 8 | 2 | 4 | 2 | - |
| 3.6 | Криптографическая защита информации | 14 | 4 | 8 | 2 | - |
| **Итого:** | | **72** | **22** | **36** | **14** | **-** |

**7. Учебная (рабочая) программа повышения квалификации «Кибербезопасность и защита данных»**

Модуль 1. Нормативно-правовая база обеспечения информационной безопасности (16 час.)

Тема 1.1 Доктрина информационной безопасности Российской Федерации (2 часа)

Тема 1.2 Государственная система защиты информации (2 часа)

Тема 1.3 Защита информации ограниченного доступа (6 часов)

Тема 1.4 Нормативные акты ФСТЭК и ФСБ России (6 часов)

Модуль 2. Ответственность за нарушение требований в области информационной безопасности (14 час.)

Тема 2.1. Критерии отнесения информации к защищаемой. Понятие и виды ущерба от НСД (8 часов)

Тема 2.1 Понятие и виды ущерба от НСД. Система современного законодательства, регламентирующая вопросы защиты информации и ответственности за нарушение информационной безопасности (6 часов)

Модуль 3 Порядок организации работ по защите информации (42 часа)

Тема 3.1 Система органов по технической защите информации в Российской Федерации (4 часа)

Тема 3.2 Технические каналы утечки информации (4 часа)

Тема 3.3 Средства выявления каналов утечки информации (8 часов)

Тема 3.4 Проблема НСД к информационным системам. Защита от физического доступа, электронные замки. Защита от НСД по компьютерным сетям (4 часа)

Тема 3.5 Модели разграничения доступа к компьютерным системам (8 часов)

Тема 3.6 Криптографическая защита информации (14 часов)

**Описание практико-ориентированных заданий и кейсов**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Номер темы/модуля** | **Наименование практического занятия** | **Описание** |
| 1.1 | Защита информации ограниченного доступа | Работа с конфеденциальной информацией | Создать виртуальную фирму или предприятие. Описать все виды информации. Рассмотреть некоторую систему, использующую эту информацию.  Определить, какие нормативно-правовые акты необходимо использовать для защиты информации в данной системе. |
| 1.2 | Нормативные акты ФСТЭК и ФСБ России | Угрозы информационной безопасности | На сайте ФСТЭК России выбрать 3 угрозы информационной безопасности (УБИ). Предложить известные средства защиты |
| 2.1 | Критерии отнесения информации к защищаемой. Понятие и виды ущерба от НСД. | Классы защищенности информационной системы | Определить класс защищенности некоторой виртуальной системы и необходимые средства защиты. |
| 2.2 | Понятие и виды ущерба от НСД. Система современного законодательства, регламентирующая вопросы защиты информации и ответственности за нарушение информационной безопасности | Оценка ущерба | Рассмотреть различные виды нарушения информационной безопасности и возможные варианты ответственности за нарушения. |
| 3.2 | Технические каналы утечки информации | Поиск технических каналов утечки информации | Организация аттестации выделенного помещения по требованиям безопасности информации  Имитатор сигналов «Шиповник-2». Скоростной поисковый приемник радиосигналов «Скорпион» |
| 3.3 | Средства выявления каналов утечки информации | Работа со средствами защиты информации от утечки | Имитатор сигналов «Шиповник-2». Скоростной поисковый приемник радиосигналов «Скорпион»  Многофункциональный поисковый прибор ST-031 «Пиранья»  Система виброакустической защиты (СВАЗ) Соната ИП-2. |
| 3.4 | Проблема НСД к информационным системам. Защита от физического доступа, электронные замки. Защита от НСД по компьютерным сетям | Защита от несанкционированного доступа | Установка и настройка ПАК «Соболь»  Интеграция ПАК «Соболь» и Secret Net  Настройка видеокомплекса BestDVR-801  Dallas Lock 8.0-K программный комплекс средств защиты информации в ОС семейства Windows с возможностью подключения аппаратных идентификаторов |
| 3.5 | Модели разграничения доступа к компьютерным системам | Типы моделей разграничения доступа | Виртуальная система обработки информации предприятия.  Построение дискреционной модели доступа, построение мандатной модели доступа, проектирование ролевой модели доступа. |
| 3.6 | Криптографическая защита информации | Практическая реализация криптографических схем и протоколов | Компьютерная реализация схем электронной жеребьевки и привязки к биту  Реализация пороговых схем разделения секрета и СРС для произвольной структуры доступа  Парольные схемы идентификации и схемы рукопожатия  Имитационное моделирование протоколов идентификации на основе ИСД с нулевым разглашением.  Стандарты цифровой подписи  Компьютерная реализация схем слепой подписи и скрытого канала  Имитационное моделирование схемы электронных денег с монетами одинакового достоинства |

**8.Оценочные материалы по образовательной программе**

**8.1. Вопросы тестирования по модулям**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ модуля** | **Вопросы входного тестирования** | **Вопросы промежуточного тестирования** | **Вопросы итогового тестирования** |
| 1 | - В чем заключается основная причина потерь информации, связанной с ПК?  - Как называется потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьих-нибудь данных? | Опрос по выполненным практическим занятиям | 1. К каким последствиям может привести утрата конфиденциальной информации. 2. От кого Вы защищаете конфиденциальную информацию. 3. Что называется коммерческой тайной? 4. Что такое служебная тайна? 5. Что представляет профессиональная тайна? 6. Что такое информация ограниченного распространения? 7. Каковы виды доступа к информации? 8. Что такое персональные данные? 9. Что такое конфиденциальная информация, государственная и ком­мерческая тайна? 10. Назовите три категории ценности коммерческой информации. 11. Что такое товарная ценность информации и каковы пути ее полу­чения? 12. На основе, каких документов проводится анализ информационных активов предприятия? 13. Какие виды информации ограниченного доступа Вы знаете? Перечислите их. 14. Что такое Коммерческая тайна? Что нельзя отнести к коммерческой тайне? 15. Что такое служебная информация? Какие виды информации Вы можете отнести к служебной тайне? 16. Что такое профессиональная тайна? Какие виды информации Вы можете отнести к профессиональной тайне? 17. Что такое интеллектуальная собственность? Какие виды информации Вы можете отнести к интеллектуальной собственности? 18. Что такое активы предприятия? Что такое информационные активы? Как правильно их проанализировать? 19. Понятие и виды информации, защищаемой законодательством Российской Федерации. Основные концептуальные положения системы защиты информации. 20. Правовое регулирование технологического обмена. Защита интеллектуальной собственности. Критерии ценности документов. 21. Предпосылки к разглашению сведений, составляющих коммерческую тайну. Экспертиза ценности документов. 22. Назовите основные мероприятиями по защите от разглашения конфиденциальной информации. |
| **2** | **-** Что такое несанкционированный доступ (нсд)?  **-**Что понимают под информационной безопасностью? | Опрос по выполненным практическим занятиям | * 1. Классификация угроз информационной безопасности объекта   2. Какая информация является охраняемой внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности?   3. Кто может быть владельцем защищаемой информации?   4. Какие сведения на территории РФ могут составлять коммерческую тайну? Какие секретные сведения входят в понятие «коммерческая тайна»?   5. В каком нормативном акте говорится о формировании и защите информационных ресурсов как национального достояния?   6. На какую структуру возложены организационные, коммерческие и технические вопросы использования информационных ресурсов страны   7. На каком уровне защиты информации создаются комплексные системы защиты информации?   8. Какие существуют наиболее общие задачи защиты информации на предприятии?   9. Какие меры и методы защиты секретной или конфиденциальной информации в памяти людей не являются основными?   10. В каком документе содержаться основные требования к безопасности информационных систем в США?   11. Какое определение соответствует термину «Аутентификация»?   12. Какое требование относится к термину «Подотчетность»?   13. Уровни безопасности системы. |
| **3** | Какие виды технической разведки (по месту размещения аппаратуры) вы знаете?  **-** Что такое криптология? | Опрос по выполненным практическим занятиям | * 1. Назначение и основные возможности поисковый прибор ST-031 «Пиранья».   2. Основные технические данные и характеристики прибора ST-031 «Пиранья».   3. Комплект прибора ST-031 «Пиранья».   4. Режимы работы поисковый прибор ST-031 «Пиранья».   5. Охарактеризовать режим высокочастотный детектор-частотомер (особенности работы, отображение результатов, частотный диапазон, виды модуляций и совместная работа с другими устройствами ТЗИ).   6. Управление прибором ST-031 «Пиранья» в режиме высокочастотного детектора-частотомера. Подготовку ST031 к работе в режим в режиме высокочастотного детектора-частотомера.   7. Базовая дискреционная ДП-модель.   8. ДП-модель без кооперации доверенных и недоверенных субъектов.   9. Мандатная ДП-модель.   10. Модель мандатного ролевого управления доступом.   Мандатная сущностно-ролевая ДП-модель управления доступом и информационными потоками в операционных системах  11.Сформулируйте, в чем состоит проблема распределения ключей.  12.Как решается проблема распределения ключей в симметричных системах?  13.Изобразите схему протокола Нидхейма-Шредера. |

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

**Оценивание выполнения практических работ**

|  |  |  |
| --- | --- | --- |
| 4-балльная шкала | Показатели | Критерии |
| Отлично | 1. Полнота выполнения практического задания; 2. Своевременность выполнения задания; 3. Последовательность и рациональность выполнения задания; 4. Самостоятельность решения; 5. и т.д. | Задание выполнено самостоятельно. При этом составлен правильный алгоритм решения задания, в логических рассуждениях, в выборе методов и средств. |
| Хорошо | Задание выполнено с помощью преподавателя. При этом составлен правильный алгоритм решения задания, в логическом рассуждении нет существенных ошибок; правильно сделан выбор методов и средств, но допущено не более двух несущественных ошибок.. |
| Удовлетворительно | Задание выполнено с подсказками преподавателя. При этом задание понято правильно, в логическом рассуждении нет существенных ошибок, задание выполнено не полностью или в общем виде. |
| Неудовлетвори­тельно | Задание не выполнено. |

|  |  |  |
| --- | --- | --- |
| 100% шкала | 51-100% | 0-49% |
| Бинарная шкала | Зачтено | Не зачтено |

**8.3. Примеры контрольных заданий по модулям или всей образовательной программе** **«Кибербезопасность и защита данных»**

Кейс 1. Разработать систему разграничения доступа для любой модели (дискреционной, мандатной, ролевой).

Кейс 2.Построить модель нарушителя и модель угроз для некоторой информационной системы.

Кейс 3. Реализовать систему с одним из вариантов ДП-модели.

**8.4.** **тесты и обучающие задачи (кейсы), иные практико-ориентированные формы заданий.**

**Модуль 1.**

1. Что такое «Информационная безопасность»?

1. Это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.
2. Это умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним.
3. Это процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.
4. Это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам.

2. Продолжите фразу: «Обладатель информации - лицо, самостоятельно создавшее…»

1. Возможность получения информации и ее использования.
2. Комплекс программных и технических средств, предназначенных для сбора, хранения, поиска и выдачи информации по запросам.
3. Информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.
4. Умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним.

3. Основы государственной политики в области обеспечения безопасности населения Российской Федерации и защищенности критически важных и потенциально опасных объектов от угроз природного, техногенного характера и террористических актов на период до 2020 года определяют:

1. цели государственной политики в области обеспечения безопасности населения и территорий Российской Федерации от угроз природного, техногенного характера и террористических актов;
2. приоритетные направления государственной политики в области обеспечения безопасности населения и территорий Российской Федерации от угроз различного характера;
3. задачи государственной политики в области обеспечения безопасности населения и территорий Российской Федерации от угроз различного характера;
4. всё вышеперечисленное.

4. Какую главную функцию выполняет ФСБ?

1. осуществляет межотраслевую координацию и функциональное регулирование деятельности по обеспечению технической защиты информации;
2. координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации;
3. участвует в разработке и реализации мер по обеспечению информационной безопасности страны, по защите сведений, составляющих государственную тайну, в лицензировании деятельности предприятий, учреждений и организаций;
4. совершенствует законодательство для эффективного использования потенциала отрасли ИБ.

5. Какой федеральный орган осуществляет межотраслевую координацию и функциональное регулирование деятельности по обеспечению технической защиты информации не криптографическими методами?

1. ФСБ;
2. ФСТЭК;
3. Комитет по вопросам информационной безопасности;
4. Совет Безопасности Российской Федерации.

6. На какие два вида подразделяется информация в соответствии с №149-ФЗ «Об информации, информационных технологиях и о защите информации»?

1. общедоступная информация;
2. особо важная информация;
3. служебная тайна;
4. информации ограниченного доступа.

**Модуль 2**

1. Виды ответственности за правонарушения в области защиты ПДн:

1. гражданская;
2. гражданская, дисциплинарная, уголовная;
3. гражданская, дисциплинарная, административная, уголовная;
4. уголовная.

2. Статьи УКРФ определяющие ответственность за правонарушения в области защиты ПДн:

1. 272, 273, 274, 146.2;
2. 271, 273, 274, 275;
3. 271;
4. В УКРФ не предусмотрена ответственность за правонарушения в области защиты ПДн.

3. Статьи КоАП определяющие ответственность за правонарушения в области защиты ПДн:

1. 13;
2. 14;
3. 146.2;
4. В КоАП не предусмотрена ответственность за правонарушения в области защиты ПДн.

4. В соответствии со статьей 6 152-ФЗ, случае, если оператор поручает обработку персональных данных другому лицу…

1. ответственность перед субъектом персональных данных за действия указанного лица несет оператор и лицо, осуществляющее обработку персональных данных по поручению оператора;
2. ответственность перед субъектом персональных данных за действия указанного лица несет только лицо, осуществляющее обработку персональных данных по поручению оператора;
3. …ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором;
4. оператор не имеет права поручать обработку персональных данных другому лицу.

5. Условия обработки ПДн:

1. Статья 6 152-ФЗ;
2. Статья 9 152-ФЗ;
3. Статья 18 152-ФЗ;
4. Статья 14 152-ФЗ.

**Модуль3**

1. К радиоэлектронной разведке Не относится:

а) РДР - радиационная разведка;

б) РР – радиоразведка;

в) РТР - радиотехническая разведка;

г) РЛР - радиолокационная разведка.

2. Классификация перечисленных каналов утечки информации: акустический, оптиче-ский, радио- электронный (э/м, электрический), материально-вещественный

а) по физической природе носителя;

б) по информативности;

в) по времени функционирования;

г) по структуре канала.

3. Утечка информации

а) незапланированный выход жидкости, газа или сыпучих материалов за пределы хра-нилища или трубопровода;

б) несанкционированное распространение носителя с информацией от ее источника к злоумышленнику;

в) санкционированное распространение носителя с информацией от ее источника к злоумышленнику;

г) несанкционированное распространение носителя с информацией от злоумышлен-ника к ее источнику.

4. Программно-аппаратный комплекс «СИГУРД» предназначен для

а) проведения специальных исследований различных технических средств по выявлению, распознаванию и измерению сигналов их побочных электромагнитных излучений с мак-симальной степенью автоматизации процедур;

б) автоматизированного контроля побочных электромагнитных излучений и наводок, а также выявления и контроля акустоэлектрических преобразований в исследуемых техни-ческих средствах;

в) автоматического, автоматизированного и экспертного поиска сигналов ПЭМИН от проверяемых технических средств, измерения частоты и пикового значения амплитуды найденных сигналов, хранения, обработки и представления результатов поиска и измере-ний в удобном для оператора виде, и применяется на объектах сферы обороны и безопасности;

г) проведения специальных исследований технических средств на сверхнормативные по-бочные электромагнитные излучения и наводки (ПЭМИН), радиомониторинга, поиска технических каналов утечки информации и технического анализа.

5. Портативный комплект для обнаружения средств съема информации и выявления ка-налов ее утечки «ПКУ-6М» не предназначен.

а) средств съема информации с передачей сигнала по существующим проводным комму-никациям;

б) утечки речевой информации по акустическому и вибро-акустическому каналам;

в) утечки цифровой информации по сети интернет;

г) средств съема информации с передачей сигнала по оптическому каналу.

6. Обязательные свойства ЭЦП – это

а) ставится человеком

б) не ставится человеком

в) изменяется с каждым документом

г) неизменна при каждом использовании

д) ставится под важными документами

е) ставится под любыми документами

ж) возможно изменение документа с сохранением подписи

з) возможно изменение документа с сохранением подписи

7. Свойство схемы обязательств, при котором пользователь А не способен изменить содержание переданного послания, называется …

а) скрывающим

б) стойким

в) связывающим

г) фиксирующим

**8.5.Описание процедуры оценивания результатов обучения**

Каждый модуль суммарно оценивается по бинарной системе: «зачет», «незачет». Практические работы оцениваются по четырех-бальной шкале. Слушатель описывает последовательность выполнения работы, отвечает на дополнительные вопросы. При успешной сдаче практических работ слушатель допускается до итогового тестирования. По результатам тестирования выставляется оценка: «зачет», «незачет».

**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 | Влацкая Ирина Валерьевна | ОГУ, зав. кафедрой КБМОИС, канд. техн. наук, доцент | http://www.osu.ru/doc/635/kafedra/6353 | C:\Users\osugeo\Downloads\Влацкая.jpg | получено |
| 2 | Мошуров Николай Павлович | ОГУ, доцент кафедры КБМОИС | http://www.osu.ru/doc/635/kafedra/6353 | **C:\Users\osugeo\Downloads\MyDdvDEpPJA.jpg** | получено |
| 3 | Джукашев Камиль Рамилевич | ОГУ, доцент кафедры КБМОИС, канд. ф.-м. наук | http://www.osu.ru/doc/635/kafedra/6353 | C:\Users\osugeo\Downloads\Джукашев.jpg | получено |
| 4 | Ряполова Елена Ивановна | ОГУ, доцент кафедры КБМОИС, канд. пед. наук | http://www.osu.ru/doc/635/kafedra/6353 | C:\Users\osugeo\Downloads\Ряполова.jpg | получено |

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

|  |  |
| --- | --- |
| **Учебно-методические материалы** | |
| Методы, формы и технологии | Методические разработки,  материалы курса, учебная литература |
| Активные и интерактивные методы ведения занятий. | . Хорев, П. Б. Методы и средства защиты информации в компьютерных системах [Текст] :  учеб. пособие / П. Б. Хорев.- 4-е изд., стер. - М. : Академия, 2008. - 256 с. : ил. - (Высшее  профессиональное образование). - Библиогр.: с. 251-252. - ISBN 978-5-7695-5118-5.  2.  3. Девянин, П.Н. Модели безопасности компьютерных систем [Текст] : учеб. пособие для  вузов / П. Н. Девянин. - М. : Академия, 2005. - 144 с. - (Высшее профессиональное образование : ин-формационная безопасность). - Библиогр.: с. 139-140. - ISBN 5-7695-2053-1.  Смарт, Н. Криптография. – М.: Техносфера, 2006. – 528 с.  2. Спицын, В. Г. Информационная безопасность вычислительной техники [Электронный ресурс] / В. Г. Спицын – Электрон.текстовые дан. – Томск : Эль Контент, 2011. – Режим доступа: http://www.biblioclub.ru/book/208694/  3. Гультяева, Т.А.Основы теории информации и криптографии: конспект лекций [Элек-тронный ресурс] / Т.А. Гультяева; Министерство образования и науки РФ, Новосибирский государ-ственный технический университет. – Новосибирск: НГТУ, 2010. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=228963 |
|  |  |

|  |  |
| --- | --- |
| **Информационное сопровождение** | |
| Электронные  образовательные ресурсы | Электронные  информационные ресурсы |
| 1. https://moodle.osu.ru - Электронные курсы ОГУ в системе обучения moodle 2. https://openedu.ru/course/hse/DATPRO/ - «Открытое образование». Курсы, МООК:Защитаинформации.   3.Сергеева Ю. С. Защита информации. Конспект лекций. Учебное пособие [Электронный  ресурс] / Сергеева Ю. С. - А-Приор, 2011. – Режим доступа:  http://www.biblioclub.ru/index.php?page=book&id=72670 | 1. http://www.fsb.ru – сайт ФСБ РФ  2. http://www.fstec.ru – сервер ФСТЭК РФ  3. http://www.gov.ru – сервер органов государственной власти РФ  4. http://www.minsvyaz.ru – сайт министерства информационных технологий и связи РФ  5. http://www.scrf.gov.ru – сайт Совета Безопасности РФ  6. www.consultant.ru – Консультант плюс  7. https://gost.ru – Росстандарт  8. http://docs.cntd.ru – Электронный фонд правовой и нормативно-технической документа-ции  9. http://www.securrity.ru – Сайт Информационная безопасность  10. https://www.securitylab.ru – Информационный портал по информационной безопасности  11. https://securelist.ru/ - Сетевая штаб-квартира экспертов «Лаборатории Касперского»  . |

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

|  |  |
| --- | --- |
| Вид занятий | Наименование оборудования,  программного обеспечения |
| Лекционные занятия | Система MOODLE, ZOOM, TEAMS |
| Практические занятия | - Электронный замок «Соболь-DS 1992 v. 3.0»  - Система оценки защищенности выделенных помещений по виброакустическому каналу «Шепот», специальное программное обеспечение «Шепот-Интерфейс»  - Программатор «Соната-ПРГ1»  - Система оценки защищенности технических средств от утечки по каналу ПЭМИН «СИГУРД»  - Test-031 (универсальный имитатор сигналов)  - Исследовательский комплекс мультисервисных беспроводных сетей  - Специализированный стенд Имитатор электролинии с ответвлением типа «Дух-01»  - Комплекс для определения величины реального затухания «ЗОНД (ГСУ-002)»  - Комплект для активных антенн со штативом «АИ4-1», «АИРЗ-1» (НЧ антенны)  - Система виброакустического зашумления «Шорох-2»  - Комплект измерительных антенн со штативом «АИ5-0», «АИР3-2» |

ПАСПОРТ КОМПЕТЕНЦИИ

**Дополнительная профессиональная программа**

**«Кибербезопасность и защита данных»**

Федеральное государственное бюджетное образовательное учреждение

высшего профессионального образования

«Оренбургский государственный университет»

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | Наименование компетенции | готовность собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности | |
| 2. | Указание типа компетенции | Профессиональная | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | Под компетенцией понимается способность оценки информационной безопасности объекта и создание средств защиты на основе нормативно-правовой базы, современных стандартов и актуальных средств защиты информации.  Слушатель должен  Знать:  - основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации;  - основные виды политик управления доступом и информационными потоками в компьютерных системах  Уметь:  - анализировать и оценивать угрозы информационной безопасности объекта;  - применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях  Владеть:  - навыками построения формальных моделей дискреционного, мандатного, ролевого управления доступом, моделей изолированной программной среды и безопасности информационных потоков  - навыками настройки межсетевых экранов;  - методиками анализа сетевого трафика. | |
| 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.) | Знает:  основные положения законодательства Российской Федерации в области защиты информации, отечественные и зарубежные стандарты в области информационной безопасности;  - основные отечественные и зарубежные стандарты в области компьютерной безопасности;  - положения стандартов Единой системы конструкторской документации, Единой системы программной документации, основные отечественные и зарубежные стандарты в области информационной безопасности, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем  - Умеет: определяит возможные угросзы информационной безопасности  Владеет:Навыками использования стандартныз средств защиты информации |
|  | Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределён-ности, сложности.) | Знает:принципы организации систем защиты информации  Уметь:построить модель нарушителя и модель угроз  Владеть: навыками проектирования системы защиты информации на основе нормативно правовой базы ИБ |
|  | Продвинутый  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знает: типовые модели безопасности компьютерных систем  Умеет:  использовать инструменты мониторинга защищенности компьютерных систем.  Владеет:  навыками реализации моделей безопасности в рамках информационных систем. |
|  | Профессиональный  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействую-щими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки  в ситуациях повышенной сложности.) | Знает:  - действующие стандарты шифрования данных;  Умеет:  классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности и оценивать угрозы безопасности информации;  - определять класс защищенности автоматизированных систем и ее составных частей;  - организовывать экспериментально-исследовательские работы при аттестации объектов с учетом требований к уровню защищенности компьютерной системы;  анализировать выбранные средства защиты данных на соответствие отечественным и зарубежным стандартам в области компьютерной безопасности  Владеет:  навыками применения и разработки средств управления информационной безопасностью компьютерной системы |

|  |  |  |
| --- | --- | --- |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | Компетенциями коммуникации в цифровой среде |
| 6. | Средства и технологии оценки | Тесты |

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

В ВУЗе уже несколько лет реализуется обучение по схожей программе: «Техническая защита информации ограниченного доступа, не содержащей сведения составляющие государственную тайну». Программа согласована с ФСТЭК РФ.

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

Рекомендации прилагаются

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

Сценарии профессиональной траектории граждан

|  |  |
| --- | --- |
| Цели получения персонального цифрового сертификата | |
| **Текущий статус** | **Цель** |
| **Трудоустройство** | |
| состоящий на учете в Центре занятости безработный | трудоустроенный, самозанятый (фриланс), ИП/бизнесмен |
| **Развитие компетенций в текущей сфере деятельности** | |
| работающий по найму в организации, на предприятии | развитие профессиональных качеств |
| работающий по найму в организации, на предприятии | повышение заработной платы |
| работающий по найму в организации, на предприятии | смена работы без изменения сферы профессиональной деятельности |
| временно отсутствующий на рабочем месте (декрет, отпуск по уходу за ребенком и др.) | сохранение и развитие квалификации |
| **Переход в новую сферу занятости** | |
| освоение новой сферы занятости | самозанятый, ИП/бизнесмен, расширение кругозора |
| освоение смежных профессиональных областей | повышение уровня дохода, расширение профессиональной деятельности |

**VII.Дополнительная информация**

В ВУЗе реализуется обучение по схожей программе: «Информационная безопасность в органах государственной власти».

**VIII.Приложенные Скан-копии** Утвержденной рабочей программа (подпись, печать, в формате pdf)

Прилагается