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

1. **Паспорт Образовательной программы**

**«**Основы информационной безопасности для пользователей**»**

|  |  |
| --- | --- |
| **Версия программы** | 1 |
| **Дата Версии** | 01**.**10.2020 |

1. **Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет» |
| 1.2 | Логотип образовательной организации |  |
| 1.3 | Провайдер ИНН | 5612001360 |
| 1.4 | Ответственный за программу ФИО | Горутько Елена Николаевна |
| 1.5 | Ответственный должность | Заведующий сектором электронных образовательных ресурсов центра информационных технологий ОГУ |
| 1.6 | Ответственный Телефон | +7(353)2375391 |
| 1.7 | Ответственный Е-mail | gorutko@mail.osu.ru |

1. **Основные Данные**

|  |  |  |
| --- | --- | --- |
| **№** | **Название** | **Описание** |
| 2.1 | Название программы | Основы информационной безопасности для пользователей |
| 2.2 | Ссылка на страницу программы | <http://www.osu.ru/doc/5022> |
| 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 | <https://moodle.osu.ru/course/view.php?id=10506> |
| 2.4 | Уровень сложности | начальный |
| 2.5 | Количество академических часов | 72 |
|  | Практикоориентированный характер образовательной программы: не менее 50 % трудоёмкости учебной деятельности отведено практическим занятиям и (или) выполнению практических заданий в режиме самостоятельной работы (кол-во академических часов) | 52 |
| 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 | 12 000 руб.  <https://euro-register.ru/services/ucenter/kursy-obucheniya-po-zashchite-personalnykh-dannykh/>  <https://www.ed.cibit.ru/programmy-obucheniya/persdannie/>  <https://edu.softline.com/directions/bezopasnost-i-zashhita-dannyh/>  [https://nousro.ru/pk-informatsionnaya-bezopasnost.php#](https://nousro.ru/pk-informatsionnaya-bezopasnost.php) |
| 2.7 | Минимальное количество человек на курсе | 10 |
| 2.8 | Максимальное количество человек на курсе | 100 |
| 2.9 | Данные о количестве слушателей, ранее успешно прошедших обучение по образовательной программе | 26 |
| 2.10 | Формы аттестации | Тестирование |
|  | Указание на область реализации компетенций цифровой экономики, к которой в большей степени относится образовательная программа, в соответствии с Перечнем областей | Кибербезопасность и защита данных |

1. **Аннотация программы**

В последнее время мы часто слышим про информационную безопасность и это неудивительно, с развитием информационных технологий любая компания или организация может стать целью кибератаки, а также угрозы для информационной безопасности могут находиться внутри самой компании и исходить от ее сотрудников.

Данный курс предлагает познакомиться с основными понятиями информационной безопасности, угрозами и информационными атаками (кибератаками); комплексом мер и инструментов защиты данных; нормативными регламентами обеспечения безопасности информации, в том числе при обработке персональных данных. В курсе вы научитесь осуществлять защиту ПК (на примере Windows), при помощи пароля; антивируса, межсетевого экрана, использовать в своей деятельности основные способы и средства защиты электронной почты и мобильного устройства; применять основные способы защиты данных при передаче в сети Интернет.

Целью программы является ознакомление слушателей с теоретическими аспектами безопасности информации и формирование практических умений обеспечения защиты данных на рабочем месте и в личном информационном пространстве.

Задачи:

Дать представление о безопасности информации, основных угрозах и информационных атаках (кибератаках); комплексе мер и инструментов защиты данных.

Дать представление о нормативных регламентах обеспечения безопасности информации, в том числе при обработке персональных данных.

Сформировать практические умения защиты данных.

МИНОБРНАУКИ РОССИИ

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

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

|  |
| --- |
|  |

**Дополнительная профессиональная программа**

**повышения квалификации**

**«Основы информационной безопасности**

**для пользователей»**

(72 часа)

2020

## Цель реализации программы

**Целью** программы является ознакомление слушателей с теоретическими аспектами безопасности информации и формирование практических умений обеспечения защиты данных на рабочем месте и в личном информационном пространстве.

**Задачи:**

Дать представление о безопасности информации, основных угрозах и информационных атаках (кибератаках); комплексе мер и инструментов защиты данных.

Дать представление о нормативных регламентах обеспечения безопасности информации, в том числе при обработке персональных данных.

Сформировать практические умения защиты данных.

## Планируемые результаты освоения программы

Обучающийся в результате освоения программы должен совершенствовать компетенции в области обеспечения безопасности информации в рабочей среде и личном информационном пространстве.

Слушатель, освоивший программу будет:

**знать:**

– сущность и понятие информационной безопасности, характеристику ее составляющих;

– основные угрозы безопасности информации, методы и способы реализации информационных атак;

– основные нормативные документы в сфере информационной безопасности;

– основные направления применения криптографии для защиты данных: шифрование, электронная подпись;

– основные методы и средства защиты персонального компьютера и мобильного устройства от различных угроз;

**уметь:**

– распознавать потенциально вредоносные действия;

– применять средства антивирусной защиты для обеспечения безопасности ПК и мобильного устройства от проникновения вирусов и вредоносных программ;

– применять средства разграничения доступа для предотвращения попыток несанкционированного доступа к информации на ПК и мобильном устройстве;

– применять правила обеспечения безопасности информации при работе с электронной почтой, в сети Интернет и на мобильном устройстве.

**владеть:**

– навыками безопасной работы на компьютере;

– навыками безопасной работы в сети интернет;

– навыками безопасной работы с электронной почтой;

– навыками безопасной работы с мобильным устройством.

1. **Категория слушателей и требования к уровню их подготовки**

Программа повышения квалификации рассчитана на обучающихся, владеющих базовыми навыками работы на компьютере.

Программа может быть полезна всем, кто интересуется проблемой информационной безопасности.

Для освоения программы не требуется специальных знаний.

1. **Учебный план программы «Основы информационной безопасности для пользователей»**

| №  п/п | Наименование модулей/тем | Объем работы слушателя, ч. | | | | Формы контроля |
| --- | --- | --- | --- | --- | --- | --- |
| Всего часов | ЛК | ПЗ | СР |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  | **Модуль 1 Информационная безопасность: нормативно-правовой аспект, общие понятия, источники угроз, кибератаки и социальный инжиниринг** | 34 | 12 | 6 | 16 |  |
|  | Введение | 4 | 2 |  | 2 | Пробный тест |
| 1 | Тема 1. Понятие безопасности информации. Угрозы информационные атаки (кибератаки), их последствия. Комплексный подход к защите информации, обзор методов и средств защиты информации | 12 | 4 | 2 | 6 | Практические задания для СР   Тестирование. |
| 2 | Тема 2.Правовые основы безопасности информации. Защита персональных данных | 14 | 4 | 4 | 6 | Практические задания для СР  Тестирование |
| 3 | Тема 3. Социальный инжиниринг | 4 | 2 | - | 2 | Тестирование. |
|  | **Модуль 2.Методы и средства защиты информации: защита устройств и программного обеспечения, безопасное поведение пользователей** | 38 | 8 | 10 | 20 |  |
| 4 | Тема 4. Безопасность электронной почты | 8 | 2 | 2 | 4 | Кейс-задание.  Тестирование. |
| 5 | Тема 5. Безопасная работа в сети Интернет | 10 | 2 | 2 | 6 | Кейс-задание  Практическое задание для СР.  Тестирование. |
| 6 | Тема 6. Защита персонального компьютера | 12 | 2 | 4 | 6 | Кейс-задание  Практическое задание для СР.  Тестирование. |
| 7 | Тема 7. Защита мобильного устройства | 8 | 2 | 2 | 4 | Практическое задание для СР.  Тестирование. |
|  | Итого: | 72 | 20 | 16 | 36 | Итоговое тестирование. |

## Календарный учебный график

|  |  |  |
| --- | --- | --- |
|  | Календарный учебный график | Общее количество месяцев/ недель |
| Срок обучения по дополнительной профессиональной программе повышения квалификации (месяцы) | ноябрь | 1 |
| Срок обучения по дополнительной профессиональной программе повышения квалификации (недели) | 2 | 2 |
| Срок обучения по дополнительной профессиональной программе повышения квалификации (дни) | 12 |  |
| Виды занятий, предусмотренные дополнительной образовательной программой повышения квалификации | ЛК + ПЗ +СР |  |

ЛК – лекционный материал

ПЗ – практические задания

СР – самостоятельная работа

## Рабочая программа курса «Основы информационной безопасности для пользователей»

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование разделов (тем) | Содержание обучения, основные дидактические единицы | Общая трудоемкость, час |
| 1 | 2 | 3 | 4 |
| 1 | Модуль 1. Информационная безопасность: нормативно-правовой аспект, общие понятия, источники угроз, кибератаки и социальный инжиниринг | | 34 |
| 2. | Введение | Сущность и значение информации в развитии современного информационного общества, опасности и угрозы, возникающие в этом процессе, основные требования информационной безопасности. | 4 |
| 3. | Тема. 1. Понятие безопасности информации. Угрозы безопасности информации. Информационные атаки (кибератаки) и их последствия. Комплексный подход к защите информации, обзор методов и средств защиты информации | Основные понятия в области безопасности информации.  Виды защищаемой информации.  Компьютерная система как объект защиты от информационных атак  Общая характеристика уязвимостей информационной системы  Основные угрозы и атаки.  Каналы утечки информации  Источники угроз безопасности информации.  Виды защиты информации.  Методы и средства защиты информации:  Комплексный подход к защите информации, | 12 |
| 4. | Тема 2. Правовые основы безопасности информации | Нормативно-правовые основы безопасности информации.  Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. Виды конфиденциальной информации Ответственность за нарушения в сфере информационной безопасности.  Защита персональных данных. Цели и задачи защиты ПДн. Основные понятия и определения. Анализ источников угроз и объектов воздействия угроз безопасности персональных данных  Организация защиты персональных данных в организации. | 14 |
| 5. | Тема 3. Социальный инжиниринг | Понятие социального инжиниринга.  Основные этапы социального взлома.  Основные техники социального инжиниринга.  Меры противодействия | 4 |
| 6. | Модуль 2.Методы и средства защиты информации: защита устройств и программного обеспечения, безопасное поведение пользователей | | 38 |
| 7. | Тема 4. Безопасность электронной почты | Проблемы защиты электронной почты  Способы и средства защиты электронной почты  Безопасность корпоративной почты.  Электронная цифровая подпись. | 8 |
| 8. | Тема 5. Безопасная работа в сети Интернет | Защита данных при передаче в сети Интернет, протокол HTTPS. Современные протоколы аутентификации Oauth/OpenID.  Меры организации безопасной удаленной работы. Облачные сервисы и хранилища информации, угрозы и средства защиты. | 10 |
| 9. | Тема 6. Защита персонального компьютера | Защита ПК (на примере Windows). Парольная защита. Разграничение доступа. Вирусы. Антивирусы. Межсетевые экраны. Шифрование дисков. | 12 |
| 10. | Тема 7. Защита мобильного устройства | Современные угрозы для мобильных устройств и способы их защиты.  Типы вредоносного мобильного ПО. Настройка мобильных приложений.  Использование личных мобильных устройств в корпоративной среде. | 8 |

## Описание практико-ориентированных заданий и кейсов

* 1. **Практико-ориентированные задания**

Практико-ориентированные задания размещены в элементе курса задание. Решение индивидуальных заданий оформляется в виде отчета и предоставляется на проверку.

Пример задания:

|  |  |
| --- | --- |
| **Тема/модуль** | **Описание** |
| Модуль 2.  Методы и средства защиты информации: защита устройств и программного обеспечения, безопасное поведение пользователей  Тема «Защита персонального компьютера» | *«Вам необходимо придумать 3 новых пароля и проверить их на надежность на сайте Касперского*  [*https://password.kaspersky.com/ru/*](https://password.kaspersky.com/ru/)  *Сервис не учитывает, что введенный вами пароль может содержать, связанную с вами информацию и может быть легко предугадан по данным социальных сетей.*  *Не используйте в задании свои действующие пароли.»*  В отчете необходимо привести пароль и его оценку системой. Сделать выводы о правилах составления паролей. Все пароли должны быть не менее 8 символов.  Варианты пароля:  1) только цифры.  2) только буквы.  3) разные типы символов.  Пароль не должен быть интуитивно понятным, не связан с вашими персональными данными (ФИО, дата рождения и т.п.), содержать разные виды символов (цифры, буквы, символы). Придумать алгоритм быстрого запоминания пароля (парольную фразу и правило для ее применения).  Проделанную работу представить в виде файла Word с примерами, скриншотами и выводами». |

Критерии оценивания:

"Зачтено" – задание выполнено полностью, оформлено, сделаны выводы, проведен анализ правил составления паролей и выбран наиболее оптимальный вариант.

"Не зачтено" – задание выполнено не полностью, отсутствуют скриншоты результатов работы, выводы.

* 1. **Кейс-задания**

Пример кейс-задания

|  |  |
| --- | --- |
| **Тема / модуль** | **Описание** |
| Модуль 2.  Методы и средства защиты информации: защита устройств и программного обеспечения, безопасное поведение пользователей  Тема «Безопасность электронной почты» | *«В понедельник утром в фирму «Л-с» поступил звонок от провайдера. Фирме отключили доступ к сети, потому что с адреса компьютера секретаря с 18.00 до 22.00 была совершена рассылка 2000 писем.*  *Секретарь фирмы – Евгения, имеет несложный пароль, состоящий из цифр, по совету системного администратора часто меняет его, но не придумывая новый, а переставляю цифры в старом, для запоминания клеит стикеры с паролем на монитор.*  *Какие ошибки в информационном поведении сотрудницы. Как действовать в данной ситуации. Как избежать подобных ситуаций позднее?»* |

Критериями оценки выполненного кейс-задания являются:

1. Полнота решения кейса.
2. Доказательность и убедительность.
3. Форма изложения материала (свободная; своими словами; грамотность устной или письменной речи).
4. Полнота и всесторонность выводов.

Проделанную работу представить в виде файла Word

"Зачтено" – задание выполнено полностью, оформлено, сделаны выводы, проведен анализ ситуации и выбран наиболее оптимальный вариант решения.

"Не зачтено" – задание выполнено не полностью, отсутствуют анализ и выводы, по представленной ситуации.

1. **Оценочные материалы по образовательной программе**
   1. **Вопросы для самопроверки**

Вопросы, которые направлены на закрепление изученного материала. Размещены в элементе курса лекция.

Пример вопроса:

*Защитой информации называют:*

*а) деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию*

*б) получение защищаемой информации заинтересованным субъектом с нарушением правил доступа к ней*

*в) доведение защищаемой информации до неконтролируемого количества получателей информации (например, публикация информации на открытом сайте в сети Интернет или в открытой печати).*

* 1. **Вопросы для обсуждения**

Вопросы, размещены в некоторых темах курса. Обсуждение происходит в форуме.

Для этих вопросов нет правильного ответа: в них важна ваша позиция и ее аргументация.

**8.3 Вопросы тестирования**

**8.3.1 Вопросы входного тестирования модуль 1**

|  |  |
| --- | --- |
| № | Вопросы входного тестирования |
| 1 | Информация - это  **–** любые сведения, которые воспринимаются живыми организмами, электронными устройствами и другими системами, об окружающем мире, процессах, предметах и явлениях;  – это знания, передаваемые в виде сообщений, уведомлений и сигналов;  – отображённое в мышлении единство существенных свойств и отношений предметов. |
| 2 | Выберите из предложенного списка антивирусные программы:  **–** Kaspersky  – Dr.Web  – Adobe Photoshop  – Paint  – ABBYY FineReader |
| 3 | Антивирусная программа - это  **–** специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов и профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом;  – компьютерная программа, которая делает вид, что удаляет вредоносное программное обеспечение, либо, действительно удаляя вредоносное ПО, взамен устанавливает своё;  – программы, которые при распространении своих копий обязательно изменяют содержимое исполняемых файлов, при этом файлы, атакованные вирусом, в большинстве случаев полностью или частично теряют работоспособность;  –компьютерная программа, вызывающая нарушение работы других программ, порчу информации, невозможность прочитать файлы, замедление, либо нестабильность работы компьютера. |
| 4 | Из предложенного списка выберите биометрические параметры идентификации личности  – форма руки;  – сетчатка глаза;  **–голос;**  –паспорт;  – удостоверение. |
| 5 | Из предложенного списка выберите действия пользователей, представляющие угрозу информационной безопасности:  **–** пароль записывается на стикер и приклеивается к монитору;  – в качестве пароля используются личные данные;  –пользователи используют один и тот же пароль для разных ресурсов;  – для подтверждения регистрации на каком-либо ресурсе, пользователь создает резервный почтовый ящик;  – пользователь не отвечает на спамерские письма. |
| 6 | Зашитой информации называют:  **–** деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;  – получение защищаемой информации заинтересованным субъектом с нарушением правил доступа к ней;  – доведение защищаемой информации до неконтролируемого количества получателей информации (например, публикация информации на открытом сайте в сети Интернет или в открытой печати). |
| 7 | Какая из перечисленных угроз не относится к угрозам  информационной безопасности:  – жизни и здоровью конкретного человека и членам его семьи, имуществу и т.д.;  – ошибки пользователей;  – ошибки в проектировании автоматизированных систем;  – воздействия на аппаратные средства компьютерной системы;  – несанкционированные действия обслуживающего персонала. |
| 8 | Под информационной безопасностью понимают:  **–** состояние защищенности информационной среды, обеспечивающее ее формирование и развитие;  – набор документированных норм, правил и практических приемов, регулирующих;  – управление, защиту и распределение информации ограниченного доступа;  – способность обеспечения беспрепятственного доступа субъектов к интересующей их информации. |
| 9 | Выберите из предложенных вариантов самый сложный пароль  – GF67\_HJkm  –FG67\_H  –100807PL  –123987560 |
| 10 | Укажите определение компьютерных вирусов:   * компьютерная программа, вызывающая нарушение работы других программ, порчу информации, невозможность прочитать файлы, замедление, либо нестабильность работы компьютера. * программа для обнаружения нежелательных (считающихся вредоносными) программ вообще и восстановления зараженных (модифицированных) такими программами файлов; * компьютерная программа, которая делает вид, что удаляет вредоносное программное обеспечение, либо, действительно удаляя вредоносное ПО, взамен устанавливает своё. |

**8.3.2 Вопросы входного тестирования модуль 2**

На выполнение заданий дается 2 попытки. Количество вопросов 15. Итоговая оценка рассчитывается как среднее значение двух попыток.

|  |  |
| --- | --- |
|  | Модуль «Защита персонального компьютера» |
| 1 | Авторизация  **–** функция вычислительной системы, которая выполняется, когда объект пытается войти в систему, сеть;  – устанавливается, является ли объект именно тем, за кого он себя выдает, другими словами эта процедура называется проверкой подлинности объекта;  – устанавливается сфера деятельности объекта и доступные ему ресурсы. |
| 2 | Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:  – детектор;  – доктор;  – сканер;  – ревизор;  – сторож. |
| 3 | Аутентификация объекта  – функция вычислительной системы, которая выполняется, когда объект пытается войти в систему, сеть;  –устанавливается, является ли объект именно тем, за кого он себя выдает, другими словами эта процедура называется проверкой подлинности объекта;  – устанавливается сфера деятельности объекта и доступные ему ресурсы. |
| 4 | Идентификация объекта  – функция вычислительной системы, которая выполняется, когда объект пытается войти в систему, сеть;  – устанавливается, является ли объект именно тем, за кого он себя выдает, другими словами эта процедура называется проверкой подлинности объекта;  –устанавливается сфера деятельности объекта и доступные ему ресурсы. |
| 5 | Для защиты от несанкционированного доступа к программам и данным, хранящимся на компьютере, используются:   * код; * анкеты; * ярлыки; * пароли. |
| 6 | Из представленного ниже списка выберите возможные способы атаки на пароль (возможно несколько вариантов ответа):   * полный перебор; * перебор в ограниченном диапазоне; * атака по словарю; * фишинг; * один к одному. |
| 7 | Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?  – сотрудники;  – хакеры;  – атакующие;  –лица, работающие по договору. |
| 8 | По типу используемой информации биометрическая идентификация делится на:  – статические способы;  –динамические способы;  – статистические способы;  – нормативно-правовые способы. |
| 9 | По среде "обитания" вирусы делятся на:  –файловые, загрузочные, макровирусы, сетевые;  – файловые, загрузочные, черви, сетевые;  – файловые, системные, сетевые;  – системные, загрузочные, сетевые. |
| 10 | Методы борьбы с вирусами подразделяются на:  – методы слежения и обнаружения;  – методы слежения и удаления;  – методы обнаружения и удаления;  – методы обнаружения и модификации. |

**8.4 Примеры вопросов итогового тестирования**

Оцениваемый тест в конце курса. Обобщающие и практические вопросы по всем разделам для аттестации по результатам обучения. Количество вопросов 30. На выполнение заданий дается одна попытка.

|  |  |
| --- | --- |
| № | Вопросы итогового тестирования |
| 1 | Защита информации не направлена на:  –ликвидацию последствий угроз;  –предупреждение угроз;  – выявление угроз;  –обнаружение угроз. |
| 2 | Цифровая подпись используется  –для методов, позволяющих установить подлинность автора сообщения при возникновении спора относительно авторства этого сообщения  –для идентификации пользователя при входе в систему  – в вычислительных системах, в которых отсутствует взаимное доверие сторон |
| 3 | Цифровая подпись формируется на основе:  – сообщения отправителя;  – сообщения получателя;  – секретного ключа отправителя;  – секретного ключа получателя;  – получатель знает проверочную комбинацию. |
| 4 | Самый лучший способ хранения паролей в информационной системе?  – хеширование;  – вообще не сохранять;  – хранить только с включенным брандмауэром;  – архивирование. |
| 5 | Антивирус, который не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:  – детектор;  –доктор;  – сканер;  – ревизор;  – сторож. |
| 6 | Для обеспечения целостности информации в процессе ее передачи по каналам связи используется:  – электронная цифровая подпись;  – протоколы идентификации;  – шифрование данных. |
| 7 | Естественные угрозы безопасности информации вызваны:  – деятельностью человека;  – ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;  – воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;  – корыстными устремлениями злоумышленников;  – ошибками при действиях персонала. |
| 8 | Спам, который распространяет поддельные сообщения от имени банков или финансовых компаний, с целью сбора логинов, паролей и пин-кодов пользователей:  –черный пиар;  –фишинг;  –нигерийские письма;  –источник слухов;  –пустые письма. |
| 9 | К преднамеренным угрозам информационной безопасности относятся:  –несанкционированные действия обслуживающего персонала;  –несанкционированный доступ к ресурсам КС пользователей и посторонних лиц;  –воздействия на аппаратные средства КС;  –ошибки в проектировании АС;  –случайные сбои. |
| 10 | Компьютерная система состоит из  – аппаратного обеспечения;  – общесистемного программного обеспечения;  – прикладного программного обеспечения;  – сетевого программного обеспечения. |

## 8.5 Промежуточная и итоговая аттестация

Промежуточная аттестация слушателей не предусмотрена.

Положительная итоговая аттестация слушателя производится при условии выполнения текущих заданий, тестов и прохождения итогового тестирования, на основании баллов, полученных за время освоения курса:

70 – 100 баллов – зачтено

0 – 69 баллов – не зачтено.

1. **Организационно-педагогические условия реализации программы**
   1. **Кадровое обеспечение программы**

**Горутько Елена Николаевна**, канд. пед. наук, зав. сектором электронных образовательных ресурсов центра информационных технологий Оренбургского государственного университета.

**Рычкова Анастасия Александровна**, канд. пед. наук, доцент кафедры вычислительной техники и защиты информации Оренбургского государственного университета, заведующий сектором электронного обучения центра информационных технологий Оренбургского государственного университета

<http://www.osu.ru/doc/1041/kaf/6342/prep/5254>

**9.2 Рекомендуемая литература**

1. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017. — 324 c.
2. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. — Ст. Оскол: ТНТ, 2017. — 384 c.
3. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. — М.: ГЛТ, 2016. — 280 c.
4. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. — М.: Форум, 2016. — 432 c.
5. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. — М.: АРТА, 2016. — 296 c.
6. Семененко, В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. — М.: МГИУ, 2017. — 277 c.

**9.3 Программное обеспечение**

1. Пакет MS Office.
2. Операционная система Windows.
3. Интернет-браузер.

**9.4 Базы данных, информационно-справочные и поисковые системы**

1. Сайт Федеральной службы по техническому и экспортному контролю https://fstec.ru/
2. КонсультантПлюс [Электронный ресурс]: электронное периодическое издание справочная правовая система. / Разработчик ЗАО «Консультант Плюс», [1992–2017]. – Режим доступа: <http://www.consultant.ru/>
3. Портал персональных данных уполномоченного органа по защите прав субъектов персональных данных https://pd.rkn.gov.ru/
   1. **Материально-техническое обеспечение учебного курса**

Обучение проводится онлайн.

**ПАСПОРТ КОМПЕТЕНЦИИ**

**Основы информационной безопасности для пользователей**

(наименование дополнительной профессиональной образовательной

программы повышения квалификации)

ФГБОУ ВО «Оренбургский государственный университет»

(наименование организации, реализующей дополнительную профессиональную образовательную программу повышения квалификации)

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | **Наименование компетенции** | Управление информацией и данными в аспекте обеспечения их безопасности и сохранности | |
| 2. | **Указание типа компетенции** | Общекультурная/универсальная | |
| 3. | **Определение, содержание и**  **основные сущностные характеристики компетенции** | Способность понимать значение информации в развитии современного общества, определять информационные ресурсы, подлежащие защите, угрозы безопасности информации,  применять информационные технологии для поиска и обработки информации и их безопасного использования | |
|  | **Дескриптор знаний, умений и навыков по уровням** | **Уровни сформированности компетенции обучающегося** | **Индикаторы** |
|  | Поверхностно ориентируется в понятийном аппарате информационной безопасности. Анализирует структуру и содержание информационных процессов предприятия, требующих защиту.  Владеет в общих чертах навыками отнесения информации к категории защищаемой | **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). | Имеет общие представления о терминологии информационной безопасности: угрозы, нарушители, конфиденциальность, доступность, целостность, политика безопасности. |
|  | Проявляет системные знания основных видов ресурсов информации, требующих защиту, умеет классифицировать информацию предприятия, требующую защиту, владеет методикой разработки модели угроз и нарушителя и соответствующей нормативной базой разработки моделей угроз и нарушителя. | **Базовый уровень**  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, сложности.) | Использует в своей деятельности знания и умения классифицировать информацию, требующую защиту. Умеет разрабатывать модель угроз и модель нарушителя. |
|  | Знает основные методы управления информационной безопасностью в полном соответствии с нормативной базой, умеет принимать самостоятельные решения по совершенствованию системы управления ИБ.  Владеет методиками модернизации, унификации систем, средств и технологий обеспечения ИБ в соответствии с нормативными актами и документами ФСТЭК России | **Продвинутый уровень**  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Применяет методы управления информационной безопасностью в полном соответствии с нормативной базой. |
|  | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | Данная компетенция является основной, на которой базируются остальные. | |
|  | Средства и технологии оценки | Практические задания  Кейс-задания  Тестирование | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | **Наименование компетенции** | Защита устройства и безопасная работа в сети Интернет | | |
| 2. | **Указание типа компетенции** | общепрофессиональная | | |
| 3. | **Определение, содержание и основные**  **сущностные характеристики компетенции** | Способность понимать значение защиты информации на персональном компьютере и при работе в сети Интернет. | | |
| 4. | **Дескриптор знаний, умений и навыков по уровням** | **Уровни сформированности компетенции обучающегося** | **Индикаторы** | |
|  | Поверхностно ориентируется в методах и средствах защиты персонального компьютера;  Поверхностно ориентируется в антивирусных программах, парольной защите компьютера. | **Начальный уровень** | Осуществляет защиту ПК (на примере Windows), использует парольную защиту, антивирусы, межсетевые экраны | |
|  | (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции.  Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.) |
|  | Демонстрирует достаточные знания методов и средств защиты персонального компьютера;  Обосновывает использование применения того или иного метода и средства защиты персонального компьютера  Демонстрирует достаточные знания антивирусных программ, имеет представление о межсетевых экранах.  Демонстрирует достаточные знания правил парольной защиты и руководствуется ими в своей деятельности. | **Базовый уровень** |
|  | (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, сложности.) |
|  | Демонстрирует глубокие знания методов и средств защиты персонального компьютера. Способен осуществить выбор наиболее оптимального средства защиты персонального компьютера,  произвести необходимые действия в случае реальной угрозы безопасности информации.  Осуществляет настройку межсетевого экрана на своем компьютере | **Продвинутый** |
|  | (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) |
|  | Поверхностно ориентируется в способах и средствах защиты электронной почты;  имеет представление об электронной цифровой подписи,  о существовании спама; | **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.) | | Использует в своей деятельности основные способы и средства защиты электронной почты |
|  | Демонстрирует достаточные знания о способах и средствах защиты электронной почты. Обосновывает использование применения того или иного способа и средства защиты электронной почты  формулирует основные способы борьбы со спамом. | **Базовый уровень**  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределён-ности, сложности.) | |
|  | Демонстрирует глубокие знания о способах и средствах защиты электронной почты.  Способен осуществить выбор наиболее оптимального средства защиты электронной почты,  произвести необходимые действия в случае реальной угрозы безопасности информации;  осуществляет настройку электронной почты на своем компьютере;  формулирует основные способы борьбы со спамом; анализирует возможные последствия при чтении спама. | **Продвинутый**  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | |
|  | Имеет поверхностное представление об основных способах защиты данных при передаче в сети Интернет | **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.) | | Применяет основные способы защиты данных при передаче в сети Интернет |
|  | Демонстрирует достаточные знания об основных способах защиты данных при передаче в сети Интернет. | **Базовый уровень**  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределён-ности, сложности.) | |  |
|  | Демонстрирует глубокие знания об основных способах защиты данных при передаче в сети Интернет. | **Продвинутый**  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | |  |
|  | Имеет поверхностное представление об основные способы и средства защиты мобильных устройств. | **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.) | | Использует в своей деятельности основные способы и средства защиты мобильных устройств |
|  | Демонстрирует достаточные знания об основные способы и средства защиты мобильных устройств, типах вредоносного мобильного ПО. | **Базовый уровень**  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, сложности.) | |  |
|  | Демонстрирует глубокие знания об основные способы и средства защиты мобильных устройств, типах вредоносного мобильного ПО. Осуществляет настройку мобильных приложений. | **Продвинутый**  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | |  |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | Компетенция базируется на компетенции «Управление информацией и данными в аспекте обеспечения их безопасности и сохранности» | | |
| 6. | Средства и технологии оценки | Практические задания  Кейс-задания  Тестирование | | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | **Наименование компетенции** | Защита персональных данных и конфиденциальность в цифровой среде. | |
| 2. | **Указание типа компетенции** | общепрофессиональная | |
| 3. | **Определение, содержание и основные**  **сущностные характеристики компетенции** | Способность использовать нормативные правовые акты в области защиты персональных данных, обрабатывать персональные данные с соблюдением требований, установленных законодательством Российской Федерации, определять правомерность запросов различных категорий граждан и должностных лиц о предоставлении доступа к документации, в том числе содержащей персональные данные.  Понимать, как пользоваться персональной информацией и защищать ее, иметь представление о методах и средствах обеспечения информационной безопасности ПДн, их классификацию, назначение, принципы работы, и особенности применения. | |
| 4. | **Дескриптор знаний, умений и навыков по уровням** | **Уровни сформированности компетенции обучающегося** | **Индикаторы** |
|  | Демонстрирует поверхностные знания в области нормативно-правовой базы защиты персональных данных, неуверенно принимает решения по определению типа персональных данных и требований к их защите  В общих чертах умеет интерпретировать правовые положения и правила поведения, закрепленные в нормативных документах по защите ПДн.  Не в полной мере владеет навыками использования нормативных материалов по защите ПДн. | **Начальный уровень** | Определяет тип персональных данных и требования к их защите. |
|  | (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции.  Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.) |
|  | Достаточно прочные знания в области нормативно-правовой базы защиты персональных данных, уверенно принимает решения по определению типа персональных данных и требований к их защите  Умеет применять действующую законодательную базу в области защиты ПДн  Достаточно владеет методами проведения анализа защищенности ПДн объектов информатизации. | **Базовый уровень** | Способен уверенно проводить анализ защищенности ПДн объектов и систем на соответствие требованиям законодательной базы в области защиты ПДн |
|  | (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, сложности) |
|  | Демонстрирует глубокие и прочные знания в области нормативно-правовой базы защиты персональных данных, способен исчерпывающе объяснять состав ПДн, выявляет основные угрозы безопасности ПДн и пути их реализации.  Обоснованно принимает решения по определению типа персональных данных и требований к их защите. | **Продвинутый** | Проводит оценку соответствия системы защиты ПДн объектов требованиям стандартов в области ИБ.  Способен самостоятельно разрабатывать организационно-распорядительные документы по защите ПДн. |
|  | (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | Компетенция базируется на компетенции «Управление информацией и данными в аспекте обеспечения их безопасности и сохранности» | |
| 6. | Средства и технологии оценки | Практические задания  Кейс-задания  Тестирование | |

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

Имеется опыт реализации программы на базе ОГУ

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

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 |

**VII.Дополнительная информация**

**нет**

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

Прилагается