I. Паспорт Образовательной программы

**«Кибербезопасность: обеспечение психологической безопасности в киберпространстве»**

УТВЕРЖДАЮ

Генеральный директор

ООО «Учебный центр Решение»

Сухов Р.В.

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

|  |  |
| --- | --- |
| Версия программы | V1 |
| Дата Версии | 14.10.2020 |

**1. Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | OOO «Учебный центр Решение» |
| 1.2 | Логотип образовательной организации | Macintosh HD:Users:aleksejvolkov:Downloads:logo_RUC_16.jpg |
| 1.3 | Провайдер ИНН | 7801640894 |
| 1.4 | Ответственный за программу ФИО | Радченко Анна Павловна |
| 1.5 | Ответственный должность | Заместитель директора по учебным программам |
| 1.6 | Ответственный Телефон | (812) 677-0507 |
| 1.7 | Ответственный Е-mail | mail@eduvideo.ru |

**2. Основные Данные**

| № | Название | Описание |
| --- | --- | --- |
| 2.1 | Название программы | Кибербезопасность**:** обеспечение психологической безопасности в киберпространстве |
| 2.2 | Ссылка на страницу программы | https://do.eduvideo.ru/video/kiberbezopasnost-pk015/ |
| 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 | ДА |
| 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) | Для практических занятий и выполнению практических заданий в режиме самостоятельной работы предусмотрено 36 акад.часов (50% от трудоемкости учебной деятельности обучающегося). |
| 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 | 29500 рублей   1. <https://skillbox.ru/course/cybersecurity/?utm_source=advcake&utm_medium=cpa&utm_campaign=affiliate&utm_content=buyavetsgmailcom&utm_term=b4ed5217093a5bf709becc1840dd09d8&advcake_params=b4ed5217093a5bf709becc1840dd09d8&sub1=checkroi-blog> 2. <https://www.academyit.ru/courses/base_ib/> 3. <https://www.academyit.ru/courses/%D0%98%D0%91030/> |
| 2.7 | Минимальное количество человек на курсе | 10 |
| 2.8 | Максимальное количество человек на курсе | 1000 |
| 2.9 | Данные о количестве слушателей, ранее успешно прошедших обучение по образовательной программе | нет |
| 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 |

**3. Аннотация программы**

Основной целью программы является, активизировать ресурсы сопротивляемости и использовать потенциал сервисов сети Интернет в профессиональных целях, минимизируя угрозы для психического здоровья и уровня психологической безопасности личности.

Особенностью программы является формирование компетенций, необходимых для применения понятия конструктивной и деструктивной информации, понятие манипуляции, способы противодействия манипуляциям в Сети.

Также целями программы являются формирование у обучающихся ключевых компетенций по выявлению факторов риска во взаимодействии с киберпространством.

Целевые аудитории обучающихся – пользователи сети Интернет, специалисты по информационной безопасности, специалисты по интернет-маркетингу.

Программа построена от общих вопросов к частным: от определения основных понятий и постановки задач к методам и инструментам их решения. Таким образом, обучение возможно для лиц, имеющих высшее техническое образование (в том числе незаконченное). Программа является модульной, и разные категории обучающихся могут уделять разное внимание отдельным модулям и темам.

В результате освоения программы обучающиеся получат основы знаний и навыки психологически безопасного существования в киберпространстве.



Общество с ограниченной ответственностью «Учебный центр Решение»

|  |  |
| --- | --- |
|  | УТВЕРЖДАЮ  Генеральный директор  ООО «Учебный центр Решение»  Сухов Р.В. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «14» октября 2020 г. |
|  |
|  |

**Дополнительная профессиональная программа повышения квалификации**

**«Кибербезопасность: обеспечение психологической безопасности в киберпространстве»**

72 часа

**ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ**

# Цель программы

Программа позволит сформировать у слушателей знания в области корректного поведения в киберпространстве, психологических закономерностей существования человека в интернете, а также основы психологии поиска информации, риски для психического здоровья, имеющие место в киберпространстве. По завершении курса у слушателей будут сформированы навыки психологически безопасного существования в киберпространстве.

# 2. Планируемые результаты обучения:

2.1. Знание (осведомленность в областях)

2.1.1 понятие киберпространства, понятие социального интернет-сервиса, психологические закономерности существования человека в интернете; основы психологии поиска информации, понятие психологическая безопасность личности; риски для психического здоровья, имеющие место в киберпространстве.

2.1.2 понятия конструктивной и деструктивной информации, понятие манипуляции, способы противодействия манипуляциям, понятие личностной идентичности, понятие психологической сопротивляемости личности.

2.2. Умение (способность к деятельности)

2.2.1 использовать потенциал сервисов сети интернет в профессиональных целях для снижения угрозы для психического здоровья и уровня психологической безопасности личности.

2.2.2 пользоваться киберпространством в своих профессиональных целях, сохраняя личностную идентичность и не поддаваясь на манипуляции.

2.3. Навыки (использование конкретных инструментов)

2.3.1 навык сохранного взаимодействия посредством киберпространства

2.3.2 навык отделения конструктивной информации от деструктивной

2.3.3 навык психологически безопасного существования в киберпространстве

# 3. Категория слушателей

* 1. Образование: высшее техническое, в том числе незаконченное.
  2. Квалификация: требования не предъявляются.
  3. Наличие опыта профессиональной деятельности: требования не предъявляются
  4. Предварительное освоение иных дисциплин/курсов /модулей: не требуется.

# 4. Учебный план программы «Кибербезопасность: обеспечение психологической безопасности в киберпространстве»

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Модуль | Всего, час | Виды учебных занятий | | |
| лекции | практические занятия | самостоятельная работа |
|  | Основы психологии киберпространства | 24 | 24 | - | - |
|  | Ресурсы психологической сопротивляемости | 24 | 6 | 12 | 6 |
|  | Психологически безопасное существование в киберпространстве | 24 | 6 | 12 | 6 |
| Итоговая аттестация | |  | Зачет | | |

# 5. Календарный план-график реализации образовательной программы

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование учебных модулей | Трудоёмкость (час) | Сроки обучения |
|  | Основы психологии киберпространства | 24 | ноябрь 2020 |
|  | Ресурсы психологической сопротивляемости | 24 | ноябрь 2020 |
|  | Психологически безопасное существование в киберпространстве | 24 | ноябрь 2020 |
| Всего: | | 72 | (набор групп производится ежемесячно) |

**6. Учебно-тематический план программы «Кибербезопасность: обеспечение психологической безопасности в киберпространстве»**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Модуль / Тема | Всего, час | Виды учебных занятий | | | Формы контроля |
| лекции | практические занятия | самостоятельная работа |
| **1** | **Основы психологии киберпространства** | **24** | **24** | **-** | **-** | Входное тестирование |
| 1.1 | Психологическая безопасность личности | 12 | 12 | - | - |  |
| 1.2 | Психологическая сопротивляемость личности | 12 | 12 | - | - |  |
| **2** | **Ресурсы психологической сопротивляемости** | **24** | **6** | **12** | **6** |  |
| 2.1 | Киберпространство и психологическая безопасность личности | 12 | 3 | 6 | 3 |  |
| 2.2 | Психологические риски современного киберпространства | 12 | 3 | 6 | 3 | Промежуточный контроль |
| **3** | **Психологически безопасное существование в киберпространстве** | **24** | **6** | **12** | **6** |  |
| 3.1 | Правила общения в Интернете | 12 | 3 | 6 | 3 |  |
| 3.2 | Защита от онлайн-агрессии и кибер-буллинга | 12 | 3 | 6 | 3 | Итоговый контроль – зачет |

**7. Учебная (рабочая) программа повышения квалификации «Кибербезопасность: обеспечение психологической безопасности в киберпространстве»**

**Модуль 1. Основы психологии киберпространства ( 24 ч.)**

**Тема 1.1** Психологическая безопасность личности **( 12 ч.)**

Представлен анализ киберугроз, с которыми сталкиваются взрослые пользователи цифровых ресурсов. Рассмотрены наиболее востребованные на сегодняшний день классификации онлайн-рисков, обоснована необходимость их модификации с учетом вызовов современности. Введены в научный оборот новые виды угроз, специфичные для взрослых интернет-пользователей (дранк шейминг, кэтфишинг), которые ранее не рассматривались в отечественных исследованиях. Отдельное внимание уделяется угрозам, связанным с аватар-опосредованной коммуникацией в контексте многопользовательских игровых виртуальных сред. Предложена авторская классификация угроз психологической безопасности взрослых интернет-пользователей, разработанная на основе интеграции результатов отечественных и зарубежных исследований.

**Тема 1.2** Психологическая сопротивляемость личности **( 12 ч.)**

В теме раскрывается обоснование субъектного подхода как методологического основания для изучения сопротивляемости личности негативным жизненным ситуациям, определена взаимосвязь сопротивляемости как свойства личности с преобразующей активностью личности, связывающей субъектность и сопротивляемость, предложено авторское определение сопротивляемости как личностной способности человека с точки зрения свойства функциональной системы, интегрирующей различные психические функции и свойства.

**Модуль 2. Ресурсы психологической сопротивляемости ( 24 ч.)**

**Тема 2.1** Киберпространство и психологическая безопасность личности **( 12 ч.)**

Вопросы психологической защищенности человека от неблагоприятных условий социальной среды рассматриваются в русле концепции психологической безопасности. Обосновано, что одной из значимых угроз, препятствующих позитивному личностному развитию человека, является насилие. Обсуждаются базовые определения насилия и его психологические последствия. Рассмотрены факторы, обеспечивающие сопротивляемость насилию в процессе онтогенетического развития, учет которых необходим для оказания комплексной социально-психологической помощи детям и подросткам, подвергающимся насилию и жестокому обращению.

**Практическая работа – решение кейсов**

**Тема 2.2** Психологические риски современного киберпространства **( 12 ч.)**

* Нарушение конфиденциальности и вторжение в частную жизнь.
* Кража идентичности.
* Кража интеллектуальной собственности.
* Кибербуллинг, киберхарассмент и сталкинг.
* Преднамеренный обман (клевета).
* Спам.
* Вторжение в область финансовых транзакций онлайн.
* Вредоносное программное обеспечение и компьютерные вирусы.
* Инвестиционные аферы и жульничество.
* Виртуальные преступления.

**Модуль 3. Психологически безопасное существование в киберпространстве ( 24 ч.)**

**Тема 3.1** Правила общения в Интернете **( 12 ч.)**

Особенности интернет-общения, плюсы и минусы интернет-общения. Интернет-общение как способ самовыражения. Цифровой онлайн-этикет. Правила поведения в Сети.

**Практическая работа - Написание инструкции**

Сформулируйте перечень правил безопасного общения в социальных сетях, на профессиональных порталах, в мобильном общении (чаты, мессенджеры) (не менее 10 правил для каждой категории)

**Тема 3.2** Защита от онлайн-агрессии и кибер-буллинга **( 12 ч.)**

Анализируется явление кибербуллинга как комплексной проблемы социальной группы; приводятся результаты эмпирических исследований; предлагается модель оказания помощи гражданам, ставшими жертвами кибербуллинга.

**Практическая работа – решение кейсов**

**Описание практико-ориентированных заданий и кейсов**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Номер темы | Наименование практического занятия | Описание |
|  | 2.1 | Решение кейсов | См п. 8.4 |
|  | 2.2 | Промежуточный контроль – эксперимент | См п. 8.3 |
|  | 3.1 | Написание инструкции | Сформулируйте перечень правил безопасного общения в социальных сетях, на профессиональных порталах, в мобильном общении (чаты, мессенджеры) (не менее 10 правил для каждой категории) |
|  | 3.2 | Решение кейсов | См п. 8.4 |

# 8. Оценочные материалы по образовательной программе

**8.1. Вопросы тестирования по модулям**

|  |  |  |  |
| --- | --- | --- | --- |
| № модуля | Вопросы входного тестирования | Вопросы промежуточного тестирования | Вопросы итогового тестирования |
| 1 | Входное тестирование (см.п. 8.3) | - | - |
| 2 | - | Промежуточный контроль – практическая работа - эксперимент | - |
| 3 | - | - | Итоговый контроль – зачет |

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

**Итоговая аттестация**

Итоговая аттестация осуществляется в виде зачета, в ходе которого слушатель должен показать усвоение лекционного материала и приобретение практических навыков. Вопросы к зачету отражены в билетах.  Каждый билет содержит один теоретический вопрос по лекционному материалу.  Ответ осуществляется в устной форме на основании пройденного материала. При подготовке к ответу допускается формирование записей на бумаге.  Каждый слушатель выбирает случайный билет и получает время на подготовку к ответу - 10 минут. Каждый слушатель получает бумагу и ручку для подготовки ответа. На изложение устного ответа отводится 10 минут.

|  |  |
| --- | --- |
| **Вид задания / Критерий** | **Количество баллов в общей оценке** |
| Общее понимание содержания и структуры вопроса | от 1 до 40 |
| Полнота раскрытия каждого элемента структуры вопроса | от 1 до 40 |
| Владение базовой терминологией | от 1 до 20 |
| Максимальное количество баллов  – 100 | |

Итоговая аттестация считается пройденной, если общее количество баллов равно 75 или более.

* **от 1 до 75 баллов – незачет**
* **от 75 до 100 балов - зачет**

**Вопросы для подготовки к зачету**

1. Понятие киберпространства.
2. Психологические закономерности существования человека в интернете.
3. Понятия интериоризации и экстериоризации знаковой системы.
4. Понятие безопасности.
5. Критерии безопасности.
6. Виды безопасности.
7. Социальная безопасность.
8. Информационная безопасность.
9. Психологическая безопасность, ее уровни.
10. Понятие личности
11. Личность в системе социальных связей.
12. Критерии психологической безопасности личности.
13. Понятие психологическая сопротивляемость личности.
14. Понятие конструктивной информации.
15. Понятие деструктивной информации.
16. Понятие манипуляции, способы противодействия манипуляциям.
17. Понятие личностной идентичности.
18. Типы психологической сопротивляемости.
19. Социальные, средовые, природные, психические ресурсы психологической сопротивляемости.
20. Психогенные риски киберпространства

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

**Вопросы входного тестирования ( Тема 1.1)**

1. Миша утром обнаружил изменения на своей страничке в социальной сети. В последнее время он очень часто пользовался интернет - сервисами с чужих компьютеров. Поэтому он решил поменять все пароли на всех аккаунтах. Но новые пароли нужно запоминать или где-то хранить. Какой из данных способов наиболее безопасен и логичен для хранения паролей Миши?

1. Размещение текстового файла с паролями в облачном хранилище

2. Использование бесплатного менеджера паролей

3. Хранение паролей на рабочем столе домашнего компьютера

4. Хранение паролей в мобильном телефоне

2. Иванов Ваня решил подобрать наиболее безопасный пароль для своего аккаунта в сети Интернет. Какой из данных паролей будет наиболее безопасным?

1. Ivanov2001

2. 05052001vano

3. 05052001VanO

4. Ba05n05NBan2005

3. Вы получили письмо по электронной почте с адреса priz2017@mymail.abc:

«Уважаемый клиент! Поздравляем, номер вашего заказа при покупке товаров в интернет - магазине стал победителем лотереи. Перейдите по ссылке priz2015.abc и оформите получение приза».

Какое действие будет самым безопасным?

1. Перейти по ссылке в письме, чтобы получить подарок

2. Заблокировать отправителя

3. Удалить письмо

4. Написать ответное письмо, о том, что не участвовал в лотерее

4. Маша получила на электронную почту письмо с адреса medic@freemail.ru о сборе средств на лечение ее близкой подруги: «Дорогая подруга! У меня несчастье. Мне срочно нужна твоя помощь на лечение. Даже рубль мне поможет. Отправь SMS на номер 0000. Срочно!»

Какой вариант поведения Маши наиболее безопасен?

1. Отправить СMС, чтобы помочь подруге

2. Переслать письмо другим подругам

3. Обратиться в Полицию

4. Удалить письмо

5. На почтовый ящик Антона пришло письмо, содержащее угрозу для близких и родных людей. Какой вариант поведения Антона является наиболее безопасным?

1. Написать ответ, потребовав дополнительной информации

2. Переслать письмо товарищу, который умеет находить компьютер отправителя

3. Обратиться в Полицию

4. Не отвечать на письмо

*Входное тестирование проводится с целью определения уровня знаний слушателей по теме курса. Оценочные материалы не предполагаются.*

**Тема 2.2 Промежуточный контроль – практическая работа - эксперимент**

**Цель работы:** Раскрыть источники угроз, которые несет всемирная сеть.

**Задача работы:** Выявить угрозы, которые нас подстерегают при работе с Интернетом, и разработать рекомендации для безопасности.

**Объект исследования:** Безопасность вИнтернете.

**Предметисследования**: Использование правил безопасности при работе в сети Интернет студентами колледжа.

**Методы исследования:** беседа, сравнение, обобщение, анкетирование, статистическая обработка данных.

**Этапы исследования**:

* проведение социологического опроса
* обработка результатов

Составьте перечень вопросов, по которым можно судить о том, как часто опрашиваемые сталкиваются с неприятностями и опасностями в сети Интернет. Проанализируйте данные и представьте их в виде аналитического отчета.

Пример Анкеты

**1.Где вы пользуетесь интернетом чаще?**

* а) дома
* б) на работе
* в) в университете

**2.Используете интернет:**

* а) как средство общения
* б) для работы
* в) для просмотра фильмов
* г) для скачивания музыки

**3.Какой вред здоровью несет интернет?**

* а) ухудшается физическое здоровье
* б) ухудшается психическое и нравственное здоровье
* в) ухудшается культура поведения и успеваемость
* г) приносит пользу здоровью
* д) можно при знакомстве попасть на мошенников и преступников

**4. Какую информацию нельзя сообщать?**

* а) свой адрес
* б) свое имя, фамилия, отчество
* в) размер обуви, одежды
* г) свой псевдоним

**5. Ваш возраст и пол?**

* Женский
* Мужской
* До 18 лет
* после 18 лет

**Шкала оценивания**

|  |  |
| --- | --- |
| **Критерий** | **Количество баллов** |
| Задание выполнено в срок | 10 |
| Подготовлен аналитический отчет | 10 |
| Каждого элемент структуры отчета раскрыт полностью | 10 |
| Использована базовая терминология | 10 |
| Анкета, по которой проводился опрос, содержит не менее 5 вопросов | 10 |
| Опрошено не менее 30 человек | 10 |
| Статистические данные в отчете представлены в виде графиков и диаграмм | 10 |
| В отчете прослеживается логика изложения материала | 10 |
| В отчете присутствует аргументированный вывод по результатам эксперимента | 10 |
| Авторские находки по результатам эксперимента | 10 |
| Максимальное количество баллов  – 100   * до 70 баллов – работа требует доработки - незачет * от 70 балов – работа принята - зачет | |

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

Основной практикоориентированной формой работы обучающегося является выполнение им практических задач, которые обучающийся самостоятельно выявляет на своем предприятии и решает с использованием знаний, полученных в ходе обучения. Преподаватели оценивают решение этих задач у каждого обучающегося и дают рекомендации. В образовательной программе также используются кейсы.

**Кейс 1.** Сотрудница компании рассказала своему руководителю, что группа ее молодых коллег снимает на фото и видео все, что происходит в офисе. Чтобы было, что снимать, они берут личные вещи сотрудников, прячут и ждут когда те начнут их искать. Фото и видео сотрудники выкладывают в разные социальные сети. Действия руководителя?

**Кейс 2.** Заместитель директора по учебно-воспитательной работе получает обращение от родительского комитета одного из классов. В тексте обращения говорится о том, что в социальных сетях распространяется снимок, на котором виден список учеников класса и их оценки. К жалобе прилагаются скриншоты страницы социальной сети. Родители просят принять меры. Заместитель директора понимает, что фото с оценками обучающихся сделано с экрана компьютера учителя.

**Кейс 3**. К вам обратился ваш ребенок. Он рассказал, что около двух недель назад по электронной почте он получил приглашение от своего друга поиграть в Интернет-игру, доступ к которой открывается по прикрепленной ссылке. Перейдя по указанной в письме ссылке, он в появившемся окне подтвердил свое участие, нажав какую-то кнопку. Игра оказалась очень увлекательной, но спустя день на электронную почту пришло письмо с незнакомого адреса с требованием оплаты участия. Ребенок его проигнорировал, однако письма стали появляться каждый день и содержать угрозы благополучию его семьи. Со слов ребенка он должен уже около 100 000 рублей. Что предпринять не знает. Ваши действия?

**Кейс 4.** После первой четверти к директору школы обратилась мама новенькой девочки из 10 класса. Мама сообщила, что в социальной сети появилась группа под названием “Ненавижу новенькую”, к которой присоединилось 60% класса. В группе публикуются сведения, порочащие девочку. На телефон ребенку приходят sms с угрозами и требованиями покинуть класс. Ребенок уходить из класса и из школы не хочет, однако эмоциональное состояние ребенка беспокоит маму. Разговор с классным руководителям не привел к положительному результату.

**Кейс 5.** Маша получила на электронную почту письмо с адреса [medic@freemail.ru](https://infourok.ru/go.html?href=mailto%3Amedic%40freemail.ru) о сборе средств на лечение ее близкой подруги

«Дорогая подруга!

У меня несчастье. Мне срочно нужна твоя помощь на лечение. Даже рубль мне поможет. Отправь SMS на номер 0000

Срочно!»

Вопросы для обсуждения:

* Стоит ли Маше помочь подруге? Почему?
* Что вас настораживает в ситуации? Можно ли доверять подруге?
* Какие могут быть последствия?
* Какими способами Маша может обезопасить себя?

**Кейс 6.** Света заинтересовалась рекламой средства для похудения в Интернете и присоединилась к группе, в которой оно распространяется. Все участники группы хвалились результатами действия чудо-средства: «быстрое похудение», «ешь, что хочешь и худеешь», «секрет похудения надо хранить в тайне». Купить средство можно только при личной встрече на семинаре участников группы. О месте встречи Свете сообщат по СMС

Вопросы для обсуждения:

* Стоит ли Свете доверять информации в группе? Почему?
* Что вас настораживает в ситуации? Можно ли пойти на встречу?
* Какие могут быть последствия?
* Какой вариант поведения Светы наиболее безопасен?

**Кейс 7.** Вам пришло предложение о бесплатном обучении за рубежом. Требуется только оплатить 200 руб. за пересылку анкеты. Для этого требуется заполнить и отослать анкету и отправить СМС на короткий номер.

Вопросы для обсуждения:

* Стоит ли отправить СМС? Почему?
* Что вас настораживает в ситуации? Можно ли доверять приглашению?
* Какие могут быть последствия?
* Какой вариант поведения наиболее безопасен?

**Критерии оценивания кейса**

|  |  |
| --- | --- |
| **Критерий** | **Количество баллов** |
| Вопрос №1 | |
| Полнота ответа с использованием всей информации из описания ситуации, обоснованность, умение оперировать терминами и понятиями, использование теоретических моделей и концепций, представленность нескольких точек зрения на проблему, отсутствие фактических ошибок | 25 |
| Вопрос №2 | |
| Полнота ответа с использованием всей информации из описания ситуации, обоснованность, умение оперировать терминами и понятиями, использование теоретических моделей и концепций, представленность нескольких точек зрения на проблему, отсутствие фактических ошибок | 25 |
| Вопрос №3 | |
| Полнота ответа с использованием всей информации из описания ситуации, обоснованность, умение оперировать терминами и понятиями, использование теоретических моделей и концепций, представленность нескольких точек зрения на проблему, отсутствие фактических ошибок | 25 |
| Вопрос №4 | |
| Полнота ответа с использованием всей информации из описания ситуации, обоснованность, умение оперировать терминами и понятиями, использование теоретических моделей и концепций, представленность нескольких точек зрения на проблему, отсутствие фактических ошибок | 25 |
| Максимальное количество баллов  – 100   * до 70 баллов – незачет * от 70 балов – зачет | |

**8.5. Описание процедуры оценивания результатов обучения**.

Процедура оценивания результатов обучения включает в себя рассмотрение преподавателем итоговой работы обучающегося и собеседование с обучающимся для выдачи ему рекомендаций по использованию результатов обучения.

# 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 | Штылева Елена Владимировна | Международный банковский институт, преподаватель, Кафедра гуманитарных и социальных дисциплин, Департамент магистратуры и аспирантуры | https://www.ibispb.ru/sveden/employees/ | Macintosh HD:Users:aleksejvolkov:Downloads:IMG_3629.JPG | ДА |

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

|  |  |
| --- | --- |
| **Учебно-методические материалы** | |
| Методы, формы и технологии | Методические разработки,  материалы курса, учебная литература |
| Занятия проходят в форме вебинаров, онлайн-дискуссий, видеоконференций, групповой работы онлайн, самостоятельной работы слушателей, решение кейсов | *Александрова Л.А.* Концепции жизнестойкости в психологии // Сибирская психология сегодня. – Выпуск 2 / Под ред. М.Н. Горбатовой, А.В. Серого, М.С. Яницкого. – Кемерово: Кузбассвузиздат, 2004. – с. 82-90.  *Баева И.А.* Психологическая безопасность в образовании: Монография. – СПб.: Издательство «Союз», 2002. – 271 с.  *Водопьянова Н.Е., Старченкова Е.С.* Синдром эмоционального выгорания: диагностика и профилактика. – СПб.: Издательство «Питер», 2005. – 336 с.  *Маклаков А.Г.* Личностный адаптационный потенциал: его мобилизация и прогнозирование в экстремальных условиях // Психологический журнал. – № 1. – Т. 22. – 2001. – с.16-24.  *Нарушевич А.А.* О феномене сопротивляемости в современной зарубежной психологии // Вестник НГУ. – №42. – 2007. – с. 7-9.  *Bobek B.L.* Teacher resiliency: a key to career longevity // Clearing House. – March/April, 2002. – p. 202-206.  *Cherney D.S.* Psychobiological mechanisms of resilience and vulnerability: implications for successful adaptation to extreme stress // American Journal of Psychiatry. – № 2(161). – 2004. – p. 195-216.  *Cicchetti D.* Foreword // Resilience and Vulnerability: adaptation in the context of childhood adversities / S. Luthar (Ed). – Cambridge: University press, 2003. – p. xix – xxvii.  *Garmezy N.* Reflections and commentary on risk, resilience, and development // Stress, risk, and resilience in children and adolescents: Processes, mechanisms, and interventions / R. Haggerty, L. Sherrod, N. Garmezy, & M.Rutter (Eds.). – Cambridge: Cambridge University Pres, 1994. – pp. 1-18.  *Ionescu S.* La resilience et les concepts apparentes // Психологическая безопасность, устойчивость, психотравма: Сборник научных статей по материалам Первого Международного Форума (Санкт-Петербург, 5-7 июня 2006 г.) / Под общ. Ред. И.А. Баевой, Ш. Ионеску, Л.А. Регуш / Пер. Н.Л. Регуш, С.А. Чернышевой. – СПб.: Издательство «Книжный Дом», 2006. – с. 14 – 17.  *Keys C.L.M.* Risk and Resilience in Human Development: An Introduction // Research in Human Development. – 1(4). – 2004. – p. 223-227.  *Maddi S.R.* Relevance of Hardiness Assessment and Training to the Military Context // Military Psychology. – №19(1). – 2007. – p. 61-70.  *Scoville M.C.* Wartime tasks of psychiatric social workers in Great Britain // American Journal of Psychiatry. – №99 (November). – 1942. – p. 358-363.  *Velichkovsky B.B.* Primary and secondary appraisals in measuring resilience to stress // Psychology in Russia: State of the Art. – 2009. – p. 539 – 563. |

|  |  |
| --- | --- |
| **Информационное сопровождение** | |
| Электронные  образовательные ресурсы | Электронные  информационные ресурсы |
| - | *Войскунский А.Е.* Поведение в киберпространстве: психологические принципы // Человек. – 2016. - № 1. – с. 36-49. (<http://elibrary.ru/item.asp?id=25954571>) |

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

|  |  |
| --- | --- |
| Вид занятий | Наименование оборудования,  программного обеспечения |
| Лекции | Компьютер с выходом в сеть Интернет, обладающий характеристиками для бесперебойной передачи аудио и видео потока, оборудованный веб- камерой 2 МПикс, с подключенным принтером, сканером, микрофоном, колонками/наушниками не ниже, чем: процессор с тактовой частотой 1 ГГц; оперативная память 512 Мб; видеокарта с 32 Мб видеопамяти; свободное место на диске 5 Гб; возможность доступа в сеть Интернет на скорости не ниже 512 Мб/сек. |
| Практико-ориентированные задания | Компьютер с выходом в сеть Интернет, установленное ПО - MS Office |

УТВЕРЖДАЮ

Генеральный директор

ООО «Учебный центр Решение»

Сухов Р.В.

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

ПАСПОРТ КОМПЕТЕНЦИИ

дополнительной профессиональной образовательной программы повышения квалификации   
**" Кибербезопасность: обеспечение психологической безопасности в киберпространстве "**

ООО "Учебный центр Решение"

Предлагаемая программа повышения квалификации предназначена для формирования у обучающихся следующих профессиональных компетенций:

|  |  |  |
| --- | --- | --- |
| 1 | Наименование компетенции | Способность осуществлять сбор, анализ информации, осуществлять безопасное присутствие личности в киберпросторанстве |
| 2 | Указание типа компетенции | профессиональная |
| 3 | Определение, содержание и основные сущностные характеристики компетенции | Знать: понятие киберпространства, понятие социального интернет-сервиса, психологические закономерности существования человека в интернете; основы психологии поиска информации, понятие психологическая безопасность личности; риски для психического здоровья, имеющие место в киберпространстве.  Уметь: использовать потенциал сервисов сети интернет в профессиональных целях минимизируя угрозы для психического здоровья и уровня психологической безопасности личности.  Владеть: навыком сохранного взаимодействия посредством киберпространства. |
| 4 | Дескриптор знаний, умений и навыков по уровням | Психологически комфортное существование в киберпространстве |
|  | Уровень | Индикаторы |
|  | Базовый | Знать: понятия конструктивной и деструктивной информации, понятие манипуляции, способы противодействия манипуляциям, понятие личностной идентичности, понятие психологической сопротивляемости личности.  Уметь: пользоваться киберпространством в своих профессиональных целях, сохраняя личностную идентичность и не поддаваясь на манипуляции.  Владеть: навыком отделения конструктивной информации от деструктивной. |
|  | Продвинутый | Знать: основные виды психологической сопротивляемости личности, понятие фактора риска, понятие защитного фактора, ресурсы сопротивляемости, стратегии поведения в ситуации воздействия фактора риска.  Уметь: выявлять факторы риска во взаимодействии с киберпространством, активизировать ресурсы сопротивляемости в целях контроля факторов психогенного риска в киберпространстве.  Владеть: навыками психологически безопасного существования в киберпространстве. |
| 5 | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | Компетенции цифровой грамотности. |
| 6 | Средства и технологии оценки | Тесты, кейсы, выполнение практических заданий. |

В ходе освоения указанной компетенции у обучающихся также формируются следующие ключевые компетенции цифровой экономики из официального перечня:

|  |  |
| --- | --- |
| Ключевые компетенции цифровой экономики | Уровень сформированности |
| **Коммуникация и кооперация в цифровой среде.** | Продвинутый |
| **Управление информацией и данными.** | Продвинутый |
| **Критическое мышление в цифровой среде.** | Базовый |

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

- не предусмотрено

**V.Рекомендаций к программе от работодателей**: наличие не менее двух писем и/или подтверждения на цифровой платформе Государственной системы предоставления ПЦС от работодателей о рекомендации образовательной программы для реализации в рамках Государственной системы предоставления ПЦС на формирование у трудоспособного населения компетенций цифровой экономики с указанием востребованности результатов освоения программы в сфере деятельности соответствующих компаний и готовности к рассмотрению заявок наиболее успешно освоивших образовательную программу граждан на прохождение стажировки и (или) собеседования на предмет трудоустройства путем проставления отметки в профиле программы

- Данные приложены к Паспорту ОП

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

Возможные наименования вакансий работодателей:

* Менеджер (администратор) информационных систем
* Консультант по кибербезопасности

По итогам обучения возможно продолжение обучение по следующим направлениям цифровых технологий:

- Цифровой дизайн

**VII.Дополнительная информация**

**-**

**VIII.Приложенные Скан-копии**

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