1. **Паспорт Образовательной программы**

Уважаемые образовательные организации!

Вы можете преобразовать шаблон в обычный Word, удалив установленное нами закрепление полей, но сохранив общую структуру. Закрепление было сделано для удобства ОО, чтобы было понятно, где можно менять данные. А где – нет.

При внесении необходимых Вам изменений в данный шаблон, пожалуйста, сохраняйте предложенную нами структуру документа.

**«** Комплексная защита информации**»**

|  |  |
| --- | --- |
| **Версия программы** | **1** |
| **Дата Версии** | 12.10.2020 |

1. **Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | «Нижегородский государственный технический университет им. Р.Е. Алексеева»  (НГТУ) |
| 1.2 | Логотип образовательной организации |  |
| 1.3 | Провайдер ИНН | 5260001439 |
| 1.4 | Ответственный за программу ФИО | Ляхманов Дмитрий Александрович |
| 1.5 | Ответственный должность | И.о. заведующего кафедрой "Информационная безопасность вычислительных систем и сетей" |
| 1.6 | Ответственный Телефон | +7-910-105-40-92 |
| 1.7 | Ответственный Е-mail | <lyahmanov@nntu.ru> |

1. **Основные Данные**

|  |  |  |
| --- | --- | --- |
| **№** | **Название** | **Описание** |
| 2.1 | Название программы | Комплексная защита информации |
| 2.2 | Ссылка на страницу программы | https://ips.nntu.ru/content/napravleniya-obucheniya/informacionnye-tekhnologii/cont/kompleksnaya-zashhita-informacii |
| 2.3 | Формат обучения | Онлайн |
| 2.4 | Подтверждение от ОО наличия возможности реализации образовательной программы с применением электронного обучения и (или) дистанционных образовательных технологий с возможностью передачи данных в форме элементов цифрового следа | Существует возможность реализации образовательной программы полностью в дистанционном формате с применением элементов электронного обучения |
| 2.5 | Уровень сложности | Базовый |
| 2.6 | Количество академических часов | **72** |
| 2.7 | Практикоориентированный характер образовательной программы: не менее 50 % трудоёмкости учебной деятельности отведено практическим занятиям и (или) выполнению практических заданий в режиме самостоятельной работы (кол-во академических часов) | Практикоориентированный характер образовательной программы: количество учебной деятельности отведено практическим занятиям и (или) выполнению практических заданий в режиме самостоятельной работы (36 академических часов) |
| 2.8 | Стоимость обучения одного обучающегося по образовательной программе, а также предоставление ссылок на 3 (три) аналогичные образовательные программы иных организаций, осуществляющих обучение, для оценки объективности стоимости или обоснование уникальности представленной образовательной программы в случае отсутствия аналогичных образовательных программ на рынке образовательных услуг | 30 000 рублей  <https://szckzi.ru/portfolio/146> - 33 000 рублей  <https://itsecurity.ru/catalog/bt112/> - 59 000 рублей  <https://ptl-nn.ru/avtorizovannoe-obuchenie/informacionnaja-bezopasnost/obespechenie-kompleksnoj-zashhity-informacii-na-predprijatii.html> - 40 300 рублей |
| 2.9 | Минимальное количество человек на курсе | 30 |
| 2.10 | Максимальное количество человек на курсе | 200 |
| 2.11 | Данные о количестве слушателей, ранее успешно прошедших обучение по образовательной программе | При наличии |
| 2.12 | Формы аттестации | Зачет |
| 2.13 | Указание на область реализации компетенций цифровой экономики, к которой в большей степени относится образовательная программа, в соответствии с Перечнем областей | Кибербезопасность и защита данных |

1. **Аннотация программы**

Наиболее полное и содержательное описание программы, которое включает:

1) общую характеристику компетенций, качественное изменение которых осуществляется в результате обучения или которые формируются в результате освоения образовательной программы;

2) описание требований и рекомендаций для обучения по образовательной программе;

3) краткое описание результатов обучения в свободной форме, а также описание востребованности результатов обучения в профессиональной деятельности.

Ограничение по размеру: не менее 1000 символов -?

**Информационная безопасность**  – это состояние информационной системы, при котором она наименее восприимчива к вмешательству и нанесению ущерба со стороны третьих лиц. Безопасность данных также подразумевает управление рисками, которые связаны с разглашением информации или влиянием на аппаратные и программные модули защиты.

Безопасность информации, которая обрабатывается в организации, – это комплекс действий, направленных на решение проблемы защиты информационной среды в рамках компании. При этом информация не должна быть ограничена в использовании и динамичном развитии для уполномоченных лиц.

Целью дополнительной профессиональной программы «Комплексная защита информации» является изучение методов и средств управления информационной безопасностью на предприятии или промышленном объекте, а также на изучение основных подходов к разработке, реализации, эксплуатации, анализу и сопровождению систем управления информационной безопасностью. Приобретенные знания позволят обучающимся основывать свою профессиональную деятельность на процессном подходе, формировать требования к системе управления информационной безопасностью конкретного объекта, принимать участие в разработке мер обеспечения защиты информации технического и организационно-правового характера.

Задачи дисциплины:

- обучить основным принципам управления информационной безопасностью как на отдельных объектах, так и в организациях;

- разрабатывать и внедрять организационно-правовые и технические меры для предотвращения утечек конфиденциальных данных;

- проводить организационный и технический аудит информационных систем

1. ШАБЛОН ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ (ДПО)

Титульный лист программы

Название организации

Дополнительная профессиональная программа повышения квалификации

«Комплексная защита информации »

72 час.

**ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ**

**1.Цель программы**

Обеспечение комплексной защиты информации на предприятиях различных форм собственности

**2.Планируемые результаты обучения:**

2.1.Знание (осведомленность в областях)

2.1.1. угрозы и источники угроз информационной безопасности предприятий различных форм собственности;

2.1.2. цели и задачи построения политик информационной безопасности;

2.1.3. цели и задачи построения КСЗИ;

2.1.4 общие принципы проектирования КСЗИ;

2.1.5 принципы системы управления службы безопасности предприятия;

2.1.6 факторы, влияющие на организацию КСЗИ;

2.1.7 международные модели и стандарты проектирования КСЗИ.

2.2. Умение (способность к деятельности)

2.2.1. выявлять и оценивать источники угроз;

2.2.2. выявлять способы дестабилизирующего воздействия на информацию;

2.2.3. разрабатывать политику информационной безопасности автоматизированной системы;

контролировать эффективность реализации политику информационной безопасности;

2.2.4 применять российскую и международную практику построения проблемно-ориентированных КСЗИ;

2.2.5 организовать службу защиты информации в соответствии с нормативными правовыми актами, нормативными и методическими документами органов государственной власти.

2.3.Навыки (использование конкретных инструментов)

2.3.1 владение методами аудита информационной безопасности предприятий различных форм собственности;

2.3.2 методами контроля эффективности реализации политик информационной безопасности

2.3.3 методами аудита информационной безопасности предприятий различных форм собственности;

2.3.4 методами построение процессов системы управления КСЗИ.

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

* 1. Образование - Высшее
  2. Квалификация - бакалавр, магистр, специалист
  3. Наличие опыта профессиональной деятельности - Базовые знания в области защиты информации
  4. Предварительное освоение иных дисциплин/курсов /модулей - Не требуются

**4.Учебный план программы «**Комплексная защита информации **.»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль** | **Всего, час** | **Виды учебных занятий** | | |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Принципы проектирования КСЗИ уровня предприятия | 48 | 14 | 22 | 12 |
| 2 | Принципы проведения аудита информационной безопасности | 24 | 6 | 14 | 4 |
| **Итоговая аттестация** | |  | **Указывается вид (экзамен, зачёт, реферат и т.д.)** | | |
|  | | 72 | Зачет | | |

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

(дата начала обучения – дата завершения обучения) в текущем календарном году, указания на периодичность набора групп (не менее 1 группы в месяц)

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование учебных модулей** | **Трудоёмкость (час)** | **Сроки обучения** |
| **1** | Принципы проектирования КСЗИ уровня предприятия | 48 | В период 01.11.2020-15.11.2020 |
| **2** | Принципы проведения аудита информационной безопасности | 24 | В период 01.11.2020-15.11.2020 |
| **Всего:** | | 72 | 01.11.2020-15.11.2020 |

**6.Учебно-тематический план программы «**  Комплексная защита информации **»**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль / Тема** | **Всего, час** | **Виды учебных занятий** | | | **Формы контроля** |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Принципы проектирования КСЗИ уровня предприятия | 48 | 14 | 22 | 12 | зачет |
| 1.1 | Общие принципы проектирования КСЗИ | 4 | 2 |  | 2 |  |
| 1.2 | Международная практика проектирования КСЗИ | 4 | 2 |  | 2 |  |
| 1.3 | Построение процессов системы управления информационной безопасности | 15 | 4 | 8 | 3 |  |
| 1.4 | Управление КСЗИ в условиях чрезвычайных ситуаций | 15 | 4 | 8 | 3 |  |
| 1.5 | Российская практика построения проблемно-ориентированных КСЗИ | 10 | 2 | 6 | 2 |  |
| 2 | Принципы проведения аудита информационной безопасности | 24 | 6 | 14 | 4 | зачет |
| 2.1 | Аудит информационной безопасности | 10 | 2 | 6 | 2 |  |
| 2.2 | Построение политики безопасности предприятия | 14 | 4 | 8 | 2 |  |
|  | Итого | 72 | 20 | 36 | 16 |  |

**7. Учебная (рабочая) программа повышения квалификации «**  Комплексная защита информации **»**

Модуль 1. Принципы проектирования КСЗИ уровня предприятия (48 часов)

Тема 1. Общие принципы проектирования КСЗИ (8 часов)

1.1. Определение и нормативное закрепление состава защищаемой информации

1.2. Определение объектов защиты

1.3. Выявление и оценка источников угроз, способов и результатов дестабилизирующего воздействия на информацию

1.4. Моделирование КСЗИ

1.5. Технологическое и организационное построение КСЗИ

1.6. Материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ

1.7. Проектная документация КСЗИ (8 часов)

Тема 2. Международная практика проектирования КСЗИ

2.1. Процессный подход к управлению сетевой и информационной инфраструктурой.

2.2. Способы контроля и проверки процессов и систем

2.3. Модель Деминга и ITIL

2.4. Библиотека ITIL и подход ITSM

2.5. Стандарт ГОСТ Р ИСО/МЭК 17799:2005

2.6. Подход COBIT

2.7. Внедрение лучших практик ISO 17799, ITIL, cobit

2.8. Подход Microsoft к управлению сетевой и информационной инфраструктурой

2.9. Общие критерии безопасности информационных технологий (12 часов)

Тема 3. Построение процессов системы управления информационной безопасности

3.1. Понятие СУИБ. Классификация процессов управления информационной безопасности.

3.2. Подсистема управления инцидентами

3.3. Подсистема управления информационными ресурсами и носителями конфиденциальной информации

3.4. Подсистема управления доступом к информационным ресурсам и сервисам

3.5. Подсистема управления конфигурациями и изменениями

3.6. Подсистема управления персоналом

3.7. Подсистема администрирования

3.8. Построение системы антивирусной защиты

3.9. Подсистема резервного копирования и восстановления

3.10. Подсистема анализа защищённости

3.11. Подсистема управления обновлениями

3.12. Подсистема обращения с критичными технологиями

3.13. Документирование процессов СУИБ

Тема 4. Управление КСЗИ в условиях чрезвычайных ситуаций (8 часов)

4.1. Понятие и основные виды чрезвычайных ситуаций

4.2. Планирование обеспечения бесперебойной деятельности организации в случае нештатных ситуаций

Тема 5. Российская практика построения проблемно-ориентированных КСЗИ (10 часов)

5.1. Проектирование защищенных ИСПДн

5.2. Проектирование банковских КСЗИ

Модуль 2. Принципы проведения аудита информационной безопасности (24 часа)

Тема 2.1 Аудит информационной безопасности (12 часов)

2.1.1. Общие положения

2.1.2. Методика информационного обследования объектов аудита

2.1.3. Инструментальная проверка защищенности информационной системы

2.1.4. Аудит ИБ государственных структур

Тема 2.2 Построение политики безопасности предприятия (12 часов)

2.2.1 Реализация общей политики информационной безопасности предприятия

2.2.2 Реализация частных политик информационной безопасности автоматизированной системы

**Описание практико-ориентированных заданий и кейсов**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Номер темы/модуля** | **Наименование практического занятия** | **Описание** |
| 1 | Построение процессов системы управления информационной безопасности | Настройка средств предотвращения утечки конфиденциальной информации | Изучение методов и средств предотвращения утечки информации по техническим каналам и информационным сетям |
| 2 | Построение процессов системы управления информационной безопасности | Настройка средств защиты информации | Настройка средств защиты и средств анализа защищенности web-приложений от типовых сетевых атак |
| 3 | Управление КСЗИ в условиях чрезвычайных ситуаций | Анализ сетевой защищенности | Изучение методов и средств предотвращения утечек информации по сетям передачи данных |
| 4 | Управление КСЗИ в условиях чрезвычайных ситуаций | Безопасность корпоративной почтовой службы | Изучение методов и средств обеспечения защиты систем корпоративной коммуникации |
| 5 | Российская практика построения проблемно-ориентированных КСЗИ | Защита персональных данных РФ | Настройка штатных средств защиты по требованиям защиты ПДн РФ в соответствии с требованиями ФСТЭК и ФСБ |
| 6 | Аудит информационной безопасности | Аудит информационных систем | Проведение аудита информационных систем уровня предприятия с использованием аккредитованных средств |
| 7 | Построение политики безопасности предприятия | Комплексная защита от несанкционированного доступа к информационной системе. | Применение организационно-правовых и технических мер от несанкционированного доступа к информационной системе |
| 8 | Построение политики безопасности предприятия | Построение и анализ политики безопасности предприятия | Разработка конкретных примеров политик информационной безопасности государственного предприятия или коммерческой организации |

**8.Оценочные материалы по образовательной программе**

**8.1. Вопросы тестирования по модулям**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ модуля** | **Вопросы входного тестирования** | **Вопросы промежуточного тестирования** | **Вопросы итогового тестирования** |
| **1** | 1. Под информационной безопасностью понимается…  А) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.  Б) программный продукт и базы данных должны быть защищены по нескольким направ­лениям от воздействия  В) нет правильного ответа  2.Защита информации – это..  А) комплекс мероприятий, направленных на обеспечение информационной безопасности.  Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей  В) небольшая программа для выполнения определенной задачи  3. От чего зависит информационная безопасность?  А) от пользователей информационной системы  Б) от поддерживающей инфраструктуры информационной системы  В) от информации, циркулирующей в информационной системе  4. Основные составляющие информационной безопасности:  А) целостность  Б) достоверность  В) конфиденциальность  5.Доступность – это…  А) возможность за приемлемое время получить требуемую информационную услугу.  Б) логическая независимость  В) нет правильного ответа  6. Целостность – это..  А) сохранность структуры информации  Б) непротиворечивость информации  В) защищенность от разрушения  7. Конфиденциальность – это..  А) защита от несанкционированного доступа к информации  Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов  В) описание процедур  8. Какие трудности возникают в информационных системах при конфиденциальности?  А) сведения о технических каналах утечки информации являются закрытыми  Б) на пути пользовательской криптографии стоят многочисленные технические проблемы  В) все ответы правильные  9. Угроза информационной безопасности – это…  А) потенциальная возможность определенным образом нарушить информационную безопасность  Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных  В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа  10. Атака – это…  А) попытка реализации угрозы  Б) потенциальная возможность определенным образом нарушить информационную безопасность  В) программы, предназначенные для поиска необходимых программ. | Дайте определение понятию комплексная система защиты информации.  На что направлена КСЗИ? каковы ее цели и задачи?  Какие существуют уровни мер защиты?  Перечислите принципы организации КСЗИ.  Перечислите этапы разработки КСЗИ.  Какие существуют потенциальные каналы и методы несанкционированного доступа к информации?  Какие роли (должности), как правило, должны быть созданы для кадрового обеспечения функционирования КСЗИ?  Что должна отражать модель нарушителя?  Перечислите существующие виды обеспечения КСЗИ.  Дайте определение понятию «процесс». Какова цель процессного подхода?  Какие преимущества имеет процессный подход? | Дайте определение понятию комплексная система защиты информации.  На что направлена КСЗИ? каковы ее цели и задачи?  Какие существуют уровни мер защиты?  Какие роли (должности), как правило, должны быть созданы для кадрового обеспечения функционирования КСЗИ?  Что должна отражать модель нарушителя?  Перечислите существующие виды обеспечения КСЗИ.  Дайте определение понятию «процесс». Какова цель процессного подхода?  Какие преимущества имеет процессный подход?  Что представляет собой цикл Деминга и модель PDSA?  Какова связь между циклом Деминга и библиотекой ITIL?  Какие группы процессов выделяет ITIL?  Какие принципы лежат в основе ITSM?  Перечислите уровни зрелости согласно CMMI.  Опишите сущность стандарта ISO/IEC 17799 и применения модели PDSA к процессам СУИБ/СМЗИ.  Назовите основной принцип модели управления ИТ согласно CobiT.  Каким правилам стоит следовать при внедрении лучших практик ITIL, CobiT, ISO/IEC 17799.  На чем основан подход Microsoft (MSM) к управлению сетевой и информационной инфраструктурой? В чем заключается характерное отличие MSM от ITIL?  Что определяет стандарт ГОСТ Р ИСО/МЭК 15408?  На какие государственные службы возложены полномочия контроля и надзора в области обеспечения безопасности персональных данных? Каковы функции данных гос. служб в рамках указанных полномочий?  Что должно быть обеспечено в ИСПДн в части защиты ПДн?  Какие нормативно-методические документы, которые регламентируют вопрос защиты ПДн?  Дайте определение категорий персональных данных.  Назовите этапы проведения классификации ИСПДн.  Какие характеристики ИСПДн используются при классификации ИСПДн?  Решение каких задач обеспечивает базовая модель угроз безопасности ПДн?  На чем основано выявление частных угроз безопасности ИСПДн?  Какие параметры используются при определении актуальности угрозы ИСПДн?  Приведите пример технических решений обеспечения безопасности ПДн.  Назовите принципы обеспечения ИБ банковских организаций.  Перечислите этапы проектирования СМЗИ банковской организации.  Приведите примеры требований стандарта PCI DSS.  На кого возлагается ликвидация ЧС согласно требованиям российского законодательства о действиях в нештатных ситуациях.  Что необходимо иметь на случай возникновения ЧС?  Каковы выгоды от составления детального плана обеспечения бесперебойной деятельности предприятия?  Перечислите варианты технических решений восстановления деятельности после бедствия.  Какие функции должны быть запланированы (учтены в плане) на случай ЧС?  Назовите стадии планирования обеспечения бесперебойной деятельности |
| **2** |  | Перечислите уровни Политики безопасности и их состав.  Перечислите состав логической цепочки, лежащей в основе моделирования процессов нарушения информационной безопасности.  Приведите примеры объективных уязвимостей.  Приведите примеры субъективных уязвимостей.  Приведите примеры случайных уязвимостей.  Перечислите типы источников угроз.  Какие существуют методы реализации угроз? | Перечислите принципы организации КСЗИ.  Перечислите этапы разработки КСЗИ.  Перечислите уровни Политики безопасности и их состав.  Перечислите состав логической цепочки, лежащей в основе моделирования процессов нарушения информационной безопасности.  Приведите примеры объективных уязвимостей.  Приведите примеры субъективных уязвимостей.  Приведите примеры случайных уязвимостей.  Перечислите типы источников угроз.  Какие существуют методы реализации угроз?  Какие существуют потенциальные каналы и методы несанкционированного доступа к информации?  Основные причины создания политик безопасности.  Основные требования и принципы, учитываемые при разработке и внедрении политики ИБ.  Как разработать политики безопасности?  Трудности внедрения политик безопасности.  Кто заинтересован в политиках безопасности?  Состав группы по разработке политик безопасности.  Примеры частных тактических политик безопасности.  Построение реестра защищаемых объектов.  Основные этапы анализа риска.  Основные разделы политики безопасности предприятия.  Действия после утверждения политики ИБ. |

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

Правильность, полнота и аргументированность при ответе на вопросы. (Зачет/Незачет) **.**

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

1. Разработка политики безопасности для органа государственного управления

3. Разработка регламента аудита для НИИ.

4. Исследование уязвимостей сети передачи данных гос. предприятия.

5. Исследование ИС на предмет наличия сетевых уязвимостей

6. Проведение мониторинга ИС государственного учреждения.

7. Проведение проверки соответствия ИС требованиям ФЗ-152 и локальным нормативным актам

и т.д. **.**

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

1. Исследование методов и средств предотвращения утечки информации по техническим каналам

2. Исследование каналов и способов предотврещения утечки по сетям передачи данных

3. Настройка средств защиты и

4. Изучение средств анализа сетевого трафика на примере снифера Wareshark

5. Исследование базовых способов прослушивания сетевого трафика с использованием ARP-подлога

6. Подготовка криптоконтейнеров и шифрование с использованием инструментов LUCKS/dm-crypt и TrueCrypt

7. Шифрование данных с помощью PGP ГОСТ

Использование и настройка OpenVPN Gost

8. Настройка средств защиты от SPAM и SPIM для отдельных вычислительных узлов

Настройка и тестирование средств SIEM на примере Splunk

9. Проведение аудита АИС на основе 1С

10.Разработка политик информационной безопасности для типовых организаций различного типа **.**

**8.5.**  описание процедуры оценивания результатов обучения

Зачет, итоговый проект **.**

**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** | Ляхманов Дмитрий Александрович | НГТУ им Р.Е. Алексеева, к.т.н., доцент |  | C:\Users\ИПС\Downloads\Ляхманов.png | V |
| **2** | Карпычев Владимир Юрьевич | НГТУ им Р.Е. Алексеева, д.т.н., профессор |  |  | V |
| 3 | Капранов Сергей Николаевич | НГТУ им Р.Е. Алексеева, к.т.н., доцент |  | C:\Users\ИПС\Downloads\Капранов.jpg | V |

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

|  |  |
| --- | --- |
| **Учебно-методические материалы** | |
| Методы, формы и технологии | Методические разработки,  материалы курса, учебная литература |
| Лекции с мультимедийным сопровождением | Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2019. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/433715 (дата обращения: 11.10.2019). |
| Практические занятия c мультимедийным сопровождением | Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/422772 (дата обращения: 16.12.2019). |

|  |  |
| --- | --- |
| **Информационное сопровождение** | |
| Электронные  образовательные ресурсы | Электронные  информационные ресурсы |
|  | ЭБС Лань <http://e.lanbook.com/>  Договор № 28-14/19-78 от 21.12.2019 г. |
|  | ЭБС Консультант студента (электронная библиотека технического ВУЗа) <http://www.studentlibrary.ru/>  Договор № 28-14/19-77 от 19.12.2019 г. |
|  | ЭБС Юрайт <http://www.biblio-online.ru/>  Договор № от 24.07.2020г. |
|  | Информационно-справочная система «Техэксперт»  Договор № 0332100025419000101 от 30.12.2019 |
|  | Ресурсы Научно-технической библиотеки НГТУ <https://www.nntu.ru/structure/view/podrazdeleniya/nauchno-tehnicheskaya-biblioteka/resursy> |

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

|  |  |
| --- | --- |
| Вид занятий | Наименование оборудования,  программного обеспечения |
| Лекционные занятия | Microsoft Office Professional Plus 2010 Russian Open License Pack NoLevel AcademicEdition, акт предоставления прав №Us000193 от 30.07.2012 |
| Практические занятия | Операционная система Ubuntu Linux 18.01 (freeware)  - GNS3 (freeware)  - Snort (freeware)  - Wareshark (freeware)  - OpenVPN (freeware)  - Libre Office (freeware)  - Outpost Firewall Free (freeware)  - Bro Network Security Monitor (freeware)  - Security Onion (freeware)  - Radmin VPN (freeware)  - IP scanner (freeware)  - Nemesis (freeware)  - Eyercap (freeware). |
|  |  |

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

Описание перечня профессиональных компетенций, качественное изменение которых осуществляется в результате обучения.

Планируемые результаты обучения должны быть определены в виде знаний, умений, навыков и (или) опыта деятельности, характеризующих формирование/развитие компетенции(-й) в области цифровой экономики и представлены в виде Паспорта компетенций в машиночитаемом текстовом формате. Структура паспорта представлена в приложении.

ПАСПОРТ КОМПЕТЕНЦИИ

(Комплексная защита информации)

(Нижегородский государственный технический университет им. Р.Е. Алексеева)

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | Наименование компетенции | Способен формулировать комплекс мер (правила, процедуры, методы) для защиты информации | |
| 2. | Указание типа компетенции | профессиональная | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | Знать  - угрозы и источники угроз информационной безопасности предприятий различных форм собственности;  - цели и задачи построения политик информационной безопасности;  - цели и задачи построения КСЗИ;  - общие принципы проектирования КСЗИ;  - принципы системы управления службы безопасности предприятия;  - факторы, влияющие на организацию КСЗИ;  - международные модели и стандарты проектирования КСЗИ.  Уметь  - выявлять и оценивать источники угроз;  - выявлять способы дестабилизирующего воздействия на информацию;  - разрабатывать политику информационной безопасности автоматизированной системы;  - контролировать эффективность реализации политику информационной безопасности;  - применять российскую и международную практику построения проблемно-ориентированных КСЗИ;  - организовать службу защиты информации в соответствии с нормативными правовыми актами, нормативными и методическими документами органов государственной власти.  Владеть  - владение методами аудита информационной безопасности предприятий различных форм собственности;  - методами контроля эффективности реализации политик информационной безопасности  - методами аудита информационной безопасности предприятий различных форм собственности;  - методами построение процессов системы управления КСЗИ. | |
| 4. | Дескриптор знаний, умений и навыков по уровням | Уровни сформированности компетенции  обучающегося | Индикаторы |
|  | Начальный уровень  (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.) | Знать  - основные угрозы и источники угроз информационной безопасности предприятий различных форм собственности;  - цели и задачи построения политик информационной безопасности;  - цели и задачи построения КСЗИ;  - международные модели и стандарты проектирования КСЗИ.  Уметь  - выявлять и оценивать источники угроз;  Владеть  - методами контроля эффективности реализации политик информационной безопасности |
|  | Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределён-ности, сложности.) | Знать  - угрозы и источники угроз информационной безопасности предприятий различных форм собственности;  - цели и задачи построения политик информационной безопасности;  - цели и задачи построения КСЗИ;  - общие принципы проектирования КСЗИ;  - принципы системы управления службы безопасности предприятия;  - факторы, влияющие на организацию КСЗИ;  - международные модели и стандарты проектирования КСЗИ.  Уметь  - выявлять и оценивать источники угроз;  - выявлять способы дестабилизирующего воздействия на информацию;  - разрабатывать политику информационной безопасности предприятия;  - применять российскую практику построения проблемно-ориентированных КСЗИ;  Владеть  - владение методами аудита информационной безопасности государственных предприятий;  - методами аудита информационной безопасности государственных предприятий;  - методами построение процессов системы управления КСЗИ. |
|  | Продвинутый  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знать  - угрозы и источники угроз информационной безопасности предприятий различных форм собственности;  - цели и задачи построения политик информационной безопасности;  - цели и задачи построения КСЗИ;  - общие принципы проектирования КСЗИ;  - принципы системы управления службы безопасности предприятия;  - факторы, влияющие на организацию КСЗИ;  - международные модели и стандарты проектирования КСЗИ.  Уметь  - выявлять и оценивать источники угроз;  - выявлять способы дестабилизирующего воздействия на информацию;  - разрабатывать политику информационной безопасности автоматизированной системы;  - контролировать эффективность реализации политику информационной безопасности;  - применять российскую и международную практику построения проблемно-ориентированных КСЗИ;  - организовать службу защиты информации в соответствии с нормативными правовыми актами, нормативными и методическими документами органов государственной власти.  Владеть  - владение методами аудита информационной безопасности предприятий различных форм собственности;  - методами контроля эффективности реализации политик информационной безопасности  - методами аудита информационной безопасности предприятий различных форм собственности;  - методами построение процессов системы управления КСЗИ. |
|  | 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.) | Знать  - угрозы и источники угроз информационной безопасности предприятий различных форм собственности;  - цели и задачи построения политик информационной безопасности (предприятия, и его отдельных подразделений);  - цели и задачи построения КСЗИ;  - общие и детальные принципы проектирования КСЗИ;  - принципы системы управления службы безопасности предприятия;  - факторы, влияющие на организацию КСЗИ;  - международные модели и стандарты проектирования КСЗИ и оценивать их эффективность.  Уметь  - выявлять и оценивать источники угроз на конкретных предприятиях различных форм собственности ;  - выявлять способы дестабилизирующего воздействия на информацию;  - разрабатывать политику информационной безопасности автоматизированной системы в соответствии с хранимой и обрабатываемой информацией;  - с помощью различных методов и средств контролировать эффективность реализации политику информационной безопасности;  - применять российскую и международную практику построения проблемно-ориентированных КСЗИ наиболее эффективным способом;  - организовать службу защиты информации в соответствии с нормативными правовыми актами, нормативными и методическими документами органов государственной власти в соответствии с международной практикой.  Владеть  - владение методами аудита информационной безопасности предприятий различных форм собственности;  - методами контроля эффективности реализации политик информационной безопасности  - в совершенстве владеть методами аудита информационной безопасности предприятий различных форм собственности;  - в совершенстве владеть методами построение процессов системы управления КСЗИ. |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | Необходимо владения ПК на уровне уверенного пользователя  Знание основ информационной безопасности | |
| 6. | Средства и технологии оценки | Итоговое и промежуточное тестирование  Итоговый проект | |

**VI.Иная информация о качестве и востребованности образовательной программы** (результаты профессионально-общественной аккредитации образовательной программы, включение в системы рейтингования, призовые места по результатам проведения конкурсов образовательных программ и др.) (при наличии)

-

**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

1. Рекомендационное письмо НАПП

2.Рекомендационное письмо ООО "Сборочное оборудование ВИТРИ"

3. Рекомендационное письмо ООО "Металлист-Казаково"

4. Рекомендационное письмо АО "НЗ 70-летия Победы"

5. Рекомендационное письмо АО ПКО "Теплообменник"

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

1. Трудоустройство

2. Развитие компетенций в текущей деятельности

3. Переход в новую сферу занятости

**VII.Дополнительная информация**

-

**VIII.Приложенные Скан-копии**

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