**УТВЕРЖДАЮ**

Генеральный директор

НОЧУ ДПО ЦПК

«Учебный центр «ИнфоТеКС»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.О. Чефранова

01.08.2020 г.

**Паспорт Образовательной программы**

**«Кибербезопасность и защита корпоративных сетей»**

|  |  |
| --- | --- |
| **Версия программы** | **1** |
| **Дата Версии** | **01.08.2020** |

1. **Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | Негосударственное образовательное частное учреждение дополнительного профессионального образования центр повышения квалификации «Учебный центр «ИнфоТеКС» |
| 1.2 | Логотип образовательной организации |  |
| 1.3 | Провайдер ИНН | 7714400751 |
| 1.4 | Ответственный за программу ФИО | Климонтова Галина Николаевна |
| 1.5 | Ответственный должность | Менеджер проектов |
| 1.6 | Ответственный Телефон | +7 (495)737-61-92 (доб.5227) |
| 1.7 | Ответственный Е-mail | [Galina.Klimontova@infotecs.ru](mailto:Galina.Klimontova@infotecs.ru) |

1. **Основные Данные**

|  |  |  |
| --- | --- | --- |
| **№** | **Название** | **Описание** |
| 2.1 | Название программы | Кибербезопасность и защита корпоративных сетей |
| 2.2 | Ссылка на страницу программы | <https://infotecs-edu.ru/course/ochnoe/kurs-obespechenie-kiberbezopasnosti-s-pomoshchyu-sredstv-zashchity-informatsii-vipnet/>  Учебный материал открывается слушателю в личном кабинете. Вход в личный кабинет осуществляется по логину и паролю с сайта учебного центра. |
| 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 | Да |
| 2.5 | Уровень сложности | Продвинутый |
| 2.6 | Количество академических часов | 72 |
| 2.7 | Практикоориентированный характер образовательной программы: не менее 50 % трудоёмкости учебной деятельности отведено практическим занятиям и (или) выполнению практических заданий в режиме самостоятельной работы (кол-во академических часов) | 42 часа отведено практическим занятиям |
| 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 |
| 2.9 | Минимальное количество человек на курсе | 100 |
| 2.10 | Максимальное количество человек на курсе | 150 |
| 2.11 | Данные о количестве слушателей, ранее успешно прошедших обучение по образовательной программе | 30 |
| 2.12 | Формы аттестации | Итоговое тестирование |
| 2.13 | Указание на область реализации компетенций цифровой экономики, к которой в большей степени относится образовательная программа, в соответствии с Перечнем областей | Кибербезопасность и защита данных |

1. **Аннотация программы**

Программа предназначена для руководителей и специалисты подразделений по защите информации, подразделений информационной безопасности, подразделений информационных технологий, подразделений, ответственных за работу с персоналом, системных и сетевых администраторов, администраторов безопасности, администраторов средств защиты, контроля и управления безопасностью, ответственных за сопровождение и администрирование средств защиты информации и средств анализа защищенности автоматизированных систем.

Обучение нацелено на совершенствование следующих профессиональных компетенций:

1. Способность выполнять установку, настройку и обслуживание программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;
2. Способность администрировать систему защиты информации;
3. Способность организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации;
4. Способность принимать участие в формировании комплекса мер по обеспечению информационной безопасности, разрабатывать предложения по совершенствованию системы управления информационной безопасностью;
5. Способность организовать технологический процесс защиты информации в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Уровень образования лица, поступающего на обучение – среднее специальное или высшее образование, по направлению подготовки (специальности) в области математических и естественных наук, инженерного дела, технологий и технологических наук (в соответствии с перечнями специальностей и направлений подготовки высшего образования, утвержденными Министерством образования и науки Российской Федерации), подтвержденное документом об образовании.

Наличие указанного образования должно подтверждаться документом государственного или установленного образца.

Требования к предварительной подготовке:

* знание Linux (Unix) платформ;
* знание сервисных служб Linux;
* знание общих вопросов технологии построения виртуальных защищенных сетей.

Одним из наиболее актуальных вопросов защиты корпоративной информации на современном предприятии является защита информации от утечек. Как показали многочисленные исследования, наибольшую долю утечек составляют утечки информации, вызванные неправомерными действиями сотрудников – внутренних нарушителей, имеющих доступ к корпоративным ресурсам, служащие результатом как целенаправленных неправомерных действий, так и действий, совершенных вследствие халатности, невнимательности, низкого уровня грамотности в области информационной безопасности, незнания правил безопасности организации. Утечка информации также может быть результатом действия посторонних лиц, находящихся на территории организации и имеющих доступ к информационной инфраструктуре предприятия.

Следствием утечки информации может быть утечка персональных данных сотрудников и клиентов компании, утечка сведений, составляющих государственную тайну, утечка коммерческой тайны организации, служебных документов, информации о внутренней структуре предприятия, и др.

Почти каждая современная компания сталкивается с проблемой компьютерных угроз. Поэтому востребованность специалистов по информационной безопасности на рынке труда сегодня крайне высока.

Целью реализации программы является формирование и совершенствование у слушателей профессиональных компетенций в области защиты информации и защищенных компьютерных сетей, приобретение практических умений и навыков работы в системе защиты информации ViPNet, усовершенствование и отработка навыков мониторинга и анализа событий и инцидентов информационной безопасности в ПК "Ampire".

Слушатель, успешно завершивший обучение по программе дополнительного образования, сможет усовершенствовать свои знания и навыки в сфере информационной безопасности, организовать защиту данных на предприятии и успешно реализовать себя как специалист по кибербезопасности.

Негосударственное образовательное частное учреждение

дополнительного профессионального образования

центр повышения квалификации «Учебный центр «ИнфоТеКС»

УТВЕРЖДАЮ

Генеральный директор

НОЧУ ДПО ЦПК

«Учебный центр «ИнфоТеКС»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.О. Чефранова

01.08.2020 г.

Дополнительная профессиональная программа повышения квалификации

**«Кибербезопасность и защита корпоративных сетей»**

72 часа

**ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ**

**1.Цель программы**

Целью реализации программы является формирование у слушателей профессиональных компетенций в области защиты информации и защищенных компьютерных сетей, приобретение практических умений и навыков работы в системе защиты информации ViPNet, усовершенствование и отработка навыков мониторинга и анализа событий и инцидентов информационной безопасности.

**2.Планируемые результаты обучения:**

2.1. Знание (осведомленность в областях)

* общих принципов криптографии и особенностей криптосистемы в продуктах ViPNet;
* программных модулей системы ViPNet (Administrator, Coordinator Linux, Failover);
* современного состояния, тенденций и перспектив развития в области мониторинга и анализа событий и инцидентов информационной безопасности;
* структуры и организации мониторинга и анализа событий и инцидентов информационной безопасности в ПК «Ampire»;
* программно-аппаратного комплекса ViPNet IDS;
* принципов действия, технологии использования и методики применения защищенных сетей;
* методов организации защищенных сетей ViPNet;
* принципов работы программно-аппаратного модуля ViPNet IDS;
* методов мониторинга и анализа событий и инцидентов информационной безопасности;

2.2. Умение (способность к деятельности)

* создавать и модифицировать защищенные сети ViPNet по заданным схемам;
* обеспечивать взаимодействие всех объектов сети ViPNet между собой;
* администрировать программно-аппаратный комплекс ViPNet IDS;
* проводить мониторинг и анализ событий и инцидентов информационной безопасности в ПК «Ampire»;
* вести контроль безопасности функционирования программных и программно-аппаратных комплексов ViPNet;
* организовывать доступ к защищаемым ресурсам и наделять полномочиями пользователей (в соответствии с решением по доступу пользователей к информационным ресурсам и в объеме, соответствующем этому решению);
* проводить аудит журналов на предмет попыток НСД и прочих нарушений;
* осуществлять контроль правильности функционирования программных и программно-аппаратных модулей ViPNet;
* проводить мониторинг и анализ событий и инцидентов информационной безопасности;

2.3. Навыки (использование конкретных инструментов)

* навыки управления защищенными сетями;
* использование технологии организации VPN;
* владение методикой использования системы защиты информации ViPNet;
* владение методами управления программно-аппаратным комплексом ViPNet IDS;
* владение технологией мониторинга и анализа событий и инцидентов информационной безопасности.

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

3.1. Образование - среднее специальное или высшее образование, по направлению подготовки (специальности) в области математических и естественных наук, инженерного дела, технологий и технологических наук (в соответствии с перечнями специальностей и направлений подготовки высшего образования, утвержденными Министерством образования и науки Российской Федерации).

Наличие указанного образование должно подтверждаться документом государственного или установленного образца.

3.2. Требования к предварительной подготовке:

* знание Linux (Unix) платформ;
* знание сервисных служб Linux;
* знание общих вопросов технологии построения виртуальных защищенных сетей.

**4.Учебный план программы «Кибербезопасность и защита корпоративных сетей»**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль** | **Всего, час** | **Виды учебных занятий** | | | |
| **лекции** | **практические занятия** | | **самостоятельная работа** |
| **Предварительное тестирование** | | 1 |  | |  | 1 |
|  | Модуль 1. Администрирование системы защиты информации ViPNet (Windows&Linux) | 40 | 20 | | 20 |  |
|  | Модуль 2. Программно-аппаратный комплекс ViPNet IDS | 16 | 8 | | 8 |  |
|  | Модуль 3. Мониторинг компьютерных инцидентов в ПК «Ampire» | 12 | 1 | | 11 |  |
| **Итоговая аттестация** | | 3 | Дистанционное тестирование | | | |
|  | |  |  | | | |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование учебных модулей** | **Трудоёмкость (час)** | **Сроки обучения** |
| **Предварительное тестирование** | | 1 | До 30.10.2020 |
| **1** | Модуль 1. Администрирование системы защиты информации ViPNet (Windows&Linux) | 40 | 09.11.2020-13.11.2020 |
| **2** | Модуль 2. Программно-аппаратный комплекс ViPNet IDS | 16 | 16.11.2020-17.11.2020 |
| **3** | Модуль 3. Мониторинг компьютерных инцидентов в ПК «Ampire» | 12 | 18.11.2020-19.11.2020 |
| **Итоговая аттестация** | | 3 | 19.11.2020 |
| **Всего:** | | 72 |  |

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль / Тема** | **Всего, час** | **Виды учебных занятий** | | | **Формы контроля** |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Администрирование системы защиты информации ViPNet (Windows&Linux) | 40 | 19 | 20 |  |  |
| 1.1 | Введение в технологию ViPNet | 2 | 2 |  |  |  |
| 1.2 | Компоненты управления сети ViPNet | 8 | 5 | 3 |  |  |
| 1.3 | Особенности криптосистемы и ключевой структуры ViPNet | 8 | 4 | 4 |  |  |
| 1.4 | Организация межсетевого взаимодействия | 4 | 1 | 3 |  |  |
| 1.5 | Шлюзы безопасности ViPNet | 4 | 3 | 1 |  |  |
| 1.6 | Технология ViPNet Coordinator Linux | 6 | 2 | 4 |  |  |
| 1.7 | Принципы и правила работы кластера горячего резервирования Linux | 6 | 2 | 4 |  |  |
| 2 | Программно-аппаратный комплекс ViPNet IDS | 16 | 8 | 8 |  |  |
| 2.1 | Вводные понятия системы обнаружения вторжений | 3 | 3 |  |  |  |
| 2.2 | Основы администрирования программно-аппаратного комплекса ViPNet IDS | 13 | 5 | 8 |  |  |
| 3 | Мониторинг компьютерных инцидентов в ПК «Ampire» | 12 | 1 | 11 |  |  |
| 3.1 | Программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак «Ampire» | 1 | 1 |  |  |  |
| 3.2 | Киберучения на базе программного комплекса «Ampire» | 11 |  | 11 |  |  |

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

Модуль 1. Администрирование системы защиты информации ViPNet (Windows&Linux) (40 час.)

Тема 1.1 Введение в технологию ViPNet (2 час.)

Актуальность технологии ViPNet. Введение в технологию ViPNet. Состав и свойства ПО ViPNet. Способы и средства защиты информации. Технология построения виртуальных защищенных сетей (VPN). Логическая структура сети ViPNet.

Тема 1.2 Компоненты управления сети ViPNet (8 час.)

Общие сведения, основные функции и назначение программы ViPNet Administrator. Система управления ViPNet Policy Manager. Состав программного обеспечения. ЦУС и УКЦ. Особенности взаимодействия ЦУС и УКЦ. Основные понятия сетевого уровня. Основные понятия прикладного уровня. Разграничение доступа к конфиденциальной информации.

Тема 1.3 Особенности криптосистемы и ключевой структуры ViPNet (8 час.)

Особенности ключевой структуры сети ViPNet. Этапы формирования ключевой информации. Управление ключевой информации в процессе функционирования сетей. Последовательность установки и настройки ПО ViPNet. Основные действия администратора Ключевого центра. Основные действия администратора Удостоверяющего центра. Типовые варианты применения технологии ViPNet

Тема 1.4 Организация межсетевого взаимодействия (4 час.)

Виды межсетевых мастер-ключей (ММК). Развертывание виртуальной защищенной сети заданной конфигурации. Настройка, управление и модификация защищенной сети ViPNet

Тема 1.5 Общие сведения, основные функции и назначение программы ViPNet Coordinator. (4 час.)

Линейка программно-аппаратных комплексов ViPNet Coordinator HW. Логика взаимодействия Клиентов с Координаторами и координаторов между собой. Общие сведения и принцип работы ViPNet Coordinator как сервер –маршрутизатор и сервера ViPNet-Firewall.

Тема 1.6 Технология ViPNet Coordinator Linux (6 час.)

Состав и функции программного обеспечения ViPNet Coordinator Linux. Установка и настройки ПО ViPNet Coordinator Linux. Туннелирование IP-трафика. Виртуальные адреса в технологии ViPNet.

Тема 1.7 Принципы и правила работы кластера горячего резервирования Linux (6 час.)

Принципы работы ViPNet Failover. Настройка ПО ViPNet Failover.

Модуль 2. Программно-аппаратный комплекс ViPNet IDS (16 час.)

Тема 2.1. Вводные понятия системы обнаружения вторжений (3 час.)  
Вводные понятия и определения. Стандарты в области систем обнаружения вторжений. Требования регуляторов. Виды систем обнаружений вторжений. История разработок СОВ. Классификация СОВ.

Тема 2.2. Основы администрирования программно-аппаратного комплекса ViPNet IDS (13 час.)

Функциональность ПАК ViPNet IDS. Использование ПАК ViPNet IDS в локальной сети. Управление и настройка ПАК ViPNet IDS. Анализ сетевых атак.

Модуль 3. Мониторинг компьютерных инцидентов в ПК «Ampire» (12 час.)

Тема 3.1. Программный комплекс обучения методам обнаружения, анализа и устранения последствий компьютерных атак «Ampire» (1 час.)

Кибербезопасность. Основные понятия и определения. Общие сведения об учебно-тренировочной платформе «Ampire». Ролевая модель. Описание основного процесса проведения киберучений.

Тема 3.2. Киберучения на базе программного комплекса «Ampire» (11 час.)

Отработка сценариев «Защита баз данных предприятия», «Защита контроллера домена предприятия», «Защита данных сегмента АСУ ТП», «Защита корпоративного портала от внутреннего нарушителя».

**Описание практико-ориентированных заданий и кейсов**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Номер темы/модуля | Наименование практического занятия | Описание |
| 1.1 | 2/1 | Построение защищенной сети ViPNet | Практическое занятие в формате вебинара с выполнением задания слушателями на виртуальных машинах.  Отрабатываются навыки установки управляющего программного обеспечения, навыки построения виртуальной защищенной сети согласно заданной схеме |
| 1.2 | 3/1 | Модификация защищённой сети ViPNet | Практическое занятие в формате вебинара с выполнением задания слушателями на виртуальных машинах.  Отрабатываются навыки изменения структуры защищенной сети согласно данной схеме и обновления ключевой информации в защищенной сети. |
| 1.3 | 4/1 | Межсетевое взаимодействие | Практическое занятие в формате вебинара с выполнением задания слушателями на виртуальных машинах.  Формируются навыки организации межсетевого взаимодействия между сетями ViPNet, модификации межсетевого взаимодействия |
| 1.4 | 5/1 | Принцип работы ViPNet Coordinator как сервер – маршрутизатор и сервера ViPNet-Firewall. | Практическое занятие в формате вебинара с выполнением задания слушателями на виртуальных машинах.  Отрабатываются навыки настройки межсетевого экрана ПО ViPNet Coordinator Linux |
| 1.5 | 6/1 | Принципы работы Failover Linux. Настройка ПО Failover Linux | Практическое занятие в формате вебинара с выполнением задания слушателями на виртуальных машинах.  Отрабатываются навыки настройки системы защиты от сбоев на базе ViPNet Coordinator Linux |
| 1.6 | 1/2 | Управление и настройка ПАК ViPNet IDS | Практическое занятие в формате вебинара с выполнением задания слушателями на виртуальных машинах.  Отрабатываются навыки настройки ПАК ViPNet IDS |
| 1.7 | 2/2 | Работа с журналами ПАК ViPNet IDS. Анализ сетевых атак. | Практическое занятие в формате вебинара с выполнением задания слушателями на виртуальных машинах.  Отрабатываются навыки работы с журналами атак ПАК ViPNet IDS и анализа атак. |
| 1.8 | 1/3 | Отработка практических сценариев мониторинга и анализа событий информационной безопасности | Практическое занятие в формате вебинара с выполнением задания слушателями на виртуальных машинах.  Отрабатываются навыки мониторинга событий информационной безопасности на базе ПК «Ampire» |

**8.Оценочные материалы по образовательной программе**

**8.1. Вопросы тестирования по модулям**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ модуля** | **Вопросы входного тестирования** | **Вопросы промежуточного тестирования** | **Вопросы итогового тестирования** |
| 1 | 1. Назовите угрозы несанкционированного доступа. 2. Какие способы и средства защиты информации Вы знаете? 3. Какие виды информации с точки зрения защиты информации Вы знаете? 4. Какие виды ответственности предусмотрены за нарушение Федеральных законов в сфере ЗИ? 5. В каком случае могут быть предоставлены персональные данные сотрудника родственникам или членам его семьи? 6. Что такое головной Удостоверяющий центр? 7. Что такое точка распространения данных? 8. Что необходимо сделать администратору Удостоверяющего и ключевого центра до истечения срока действия сертификата? 9. Как осуществляется распространение списка аннулированных сертификатов (CRL)? 10. В случае каких событий сертификат считается недействительным? |  | 1. Где содержится информация об объектах сети ViPNet (узлах, пользователях, коллективах, их именах, идентификаторах, адресах, связях и т.д.)?  2. Сколько индивидуальных симметричных межсетевых мастер-ключей можно создать в УКЦ для доверенной сети?  3. Какие основные функции выполняет ПО ViPNet Client?  4. Какие сетевые фильтры обладают максимальным приоритетом?  5. В каких типах фильтров применяется «Группа узлов ViPNet»?  6. Для чего предназначена программа «Registration Point»?  7. Для чего нужна программа Publication Service?  8. Какая технология, применяемая в продуктах VPN ViPNet, обеспечивает сокрытие информации о IP-пакете при передачи его по сети?  9. Какой параметр не отображается в журнале регистрации IP пакетов?  10. Какие основные функции выполняет ПО ViPNet Coordinator?  11. Для чего предназначена программа «Контроль приложений»?  12. Требуется обновить на узлах своей сети ключи связи с доверенной сетью, что нужно для этого сделать?  13. Не проходит команда ping между двумя узлами защищенной сети. Где можно получить информацию о причине ошибки?  14. Вы в течение длительного времени не включали ViPNet Client. После запуска ViPNet отсутствует связь с некоторыми узлами защищенной сети, кроме того, в списке защищенной сети на компьютере пользователя отсутствует информация о нескольких узлах. Что нужно сделать в первую очередь?  15. Какой компонент сети ViPNet выполняет криптографические операции?  16. На каком уровне будет происходить шифрование писем в Outlook после обмена сертификатами открытых ключей ЭП с использованием ViPNet CSP?  17. Есть ли возможность у администратора ЦУСа ограничить размер файлов, передаваемых по "Файловому обмену"?  18. Можно ли изменить стартовый адрес, начиная с которого генерируются виртуальные IP-адреса?  19. На компьютере изменился IP-адрес сетевого интерфейса. Изменится ли при этом виртуальный IP-адрес?  20. Можно ли ограничить возможности пользователя по изменениям настроек своего сетевого узла? 21. Что такое "Служебный конверт" ViPNet?  22. Для чего служит ViPNet-драйвер?  23. Для чего предназначена программа ViPNet Policy Manager?  24. Для обмена шифрованным трафиком между защищенными узлами в случае, когда пакеты передаются по протоколу UDP, какой порт используется по умолчанию?  25. Для чего предназначен программно-аппаратный комплекс ViPNet IDS?  26. Пользователь сменил пароль на вход в ViPNet Клиент и забыл его. Что делать?  27. В списке узлов защищенной сети программы ViPNet Монитор напротив некоторых из узлов не стоит номер сети. Это ошибка?  28. Из доверенной сети получено два межсетевых ключа, следует назначить текущим:  29. Возможна ли установка компонентов ПО ViPNet «Администратор» - «ЦУС» и «УКЦ» на два отдельных компьютера?  30. Может ли ViPNet работать через VPN-каналы, организованные с помощью СЗИ других производителей? 31. Что нужно сделать после получения импорта из доверенной сети?  32. Какие файлы нужны для восстановления узла администратора или переноса на новый ПК?  33. Для чего предназначены ключи пользователя?  34. При создании в УКЦ ключей пользователя не формируется его сертификат ЭП. В чём причина?  35. В УКЦ произведена смена пароля пользователя узла, отправлено обновление, что произойдет на узле пользователя?  36. Что нужно сделать после того как в УКЦ закончился срок действия закрытого ключа администратора?  37. В каком приложении можно сохранить структуру сети в формате HTML?  38. Можно ли использовать внешние ключевые устройства в сети ViPNet?  39. Может ли быть несколько Администраторов программы ЦУС?  40. Можно ли в УКЦ версии 4.х создать несколько учетных записей Администраторов? 41. Может ли Администратор ЦУС запретить пользователю использовать Чат и Файловый обмен?  42. На какие узлы можно назначить роль "Policy Manager" в ViPNet Administrator версий до 4.6.4 включительно?  43. Где можно посмотреть максимальную допустимую версию ПО, которое вы можете установить?  44. Какие элементы DST-файла зашифрованы на ключах защиты?  45. С сайта ОАО «ИнфоТеКС» администратор скачал дистрибутив новой версии ПО ViPNet Клиент, но удаленно через ЦУС обновить ViPNet Клиент у него не получается. Почему?  46. Какой вид инкапсуляции будет использоваться ViPNet-драйвером, если на пути следования IP-пакетов происходит преобразование IP-адресов?  47. У пользователя в окне ПО "Контроль приложений" не активен пункт меню "Отключить контроль приложений". Почему?  48. Что такое "Роль" в терминологии ViPNet Administrator?  49. Для каких пользователей можно сгенерировать дистрибутив начальной инсталяции в ПО ViPNet?  50. Между защищенными ViPNet-сетями "А" и "В" организовано межсетевое взаимодействие. Между защищенными ViPNet-сетями "В" и "С" организовано межсетевое взаимодействие. Могут ли пользователи сети "А" отправлять письма по "Деловой почте" пользователям сети "С"?  51. Какой модуль в Координаторе реализует функцию сервера-маршрутизатора?  52. Что нужно сделать, чтобы отключить фильтрацию трафика в ViPNet Client версии 4.х?  53. Что входит в состав ViPNet Administrator?  54. Где можно установить клиентское приложение ЦУС?  55. В какой роли в ЦУС определяются полномочия для работы с программой "Контроль приложений"?  56. Какие способы создания структуры сети возможны в ЦУС?  57. Где отображается информация об установленных обновлениях на Client и Coordinator?  58. Как обеспечить корректную передачу трафика между туннелируемыми узлами и защищенными узлами ViPNet?  59. Что такое "сетевой фильтр" в терминологии ViPNet?  60. Что такое "шлюзовой координатор" в терминологии ViPNet?  61. Что произойдет, если на развёрнутом ViPNet Coordinator 4 for Linux истечёт срок действия пароля администратора сетевого узла?  62.Может ли MFTP-модуль Linux-координатора работать в клиентском режиме?  63. Можно ли на Linux-координаторе переопределить срок хранения транспортных конвертов в очереди?  64. Для чего в Linux-координаторе предназначен TCP-туннель?  65. Какие настройки необходимо выполнить для того, чтобы координатор заработал в качестве сервера IP-адресов?  66. Возможно ли использование компьютера с установленным ПО ViPNet Coordinator 4 for Linux в качестве DHCP-сервера?  67. Что необходимо сделать в первую очередь для того, чтобы ViPNet Coordinator 4 for Linux мог выполнять функцию туннелирования?  68. Каким параметром определяется хост, из-за отсутствия трафика с которым активный узел кластера принимает решение о неработоспособности своего сетевого интерфейса?  69. Что произойдёт, если для сетевого интерфейса не задана секция [adapter] в файле iplir.conf при включенной защите?  70. Каким параметром определяется защищаемая сеть, к которой подключен сетевой адаптер узла кластера?  71. За что отвечает секция [channel] в файле настроек транспортного модуля ViPNet Coordinator 4 for Linux?  72. В каком файле содержатся настройки транспортного модуля ViPNet Coordinator 4 for Linux?  73. При уже установленном ПО ViPNet Coordinator Linux решено пересобрать ядро Linux, что необходимо сделать после установки нового ядра?  74. Какой IP-адрес доступа к собственному узлу назначается в Coordinator 4 for Linux в файле iplir.conf?  75. Какое действие необходимо выполнить в первую очередь для редактирования конфигурационных файлов iplir.conf\*?  76. Какой алгоритм обновления ПО ViPNet Coordinator Linux на кластере обеспечит бесперебойную работу системы?  77. Как можно посмотреть журнал переключений серверов кластера горячего резервирования в координаторах ViPNet Linux 4.x?  78. В каком режиме загружается элемент кластера горячего резервирования после первой перезагрузки ОС после команды failover start без указания режима работы узла?  79. За что отвечает параметр «accessip» в iplir.conf в секциях [id], кроме собственной?  80. Какое значение параметра debuglevel в секции [debug] файла iplir.conf отключает ведение журнала? |
| 2 |  |  | 1. Что такое СОВ? 2. Какие уровни критичности атак различает ViPNet IDS? 3. Какие сетевые интерфейсы ViPNet IDS не нуждаются в настройке IP-адресов? 4. Что такое "неразборчивый режим" (promiscuous mode) работы сетевого интерфейса? 5. По каким каналам осуществляется передача данных с ПАК ViPNet IDS, находящегося вне доверенной зоны? 6. Сколько классов СОВ выделяет ФСТЭК? 7. Какой командой можно проверить доступность сетевого интерфейса? 8. Какой логин используется по умолчанию при управлении ViPNet IDS с помощью веб-интерфейса? 9. Какое минимальное количество задействованных сетевых интерфейсов должен имеет ViPNet IDS? 10. Может ли ViPNet IDS являться туннелируемым ресурсом? |
| 3 |  |  | 1. Какие действия входят в задачу участников группы мониторинга? 2. Какие действия входят в задачу лидера группы реагирования? 3. О каких событиях отображается информация в журнале событий ViPNet IDS NS? 4. Что такое инцидент информационной безопасности? 5. Какие виды ответственности предусмотрены законодательством РФ в области информационной безопасности? 6. Каким браузером следует пользоваться при работе с web-интерфейсом ViPNet IDS? 7. Может ли ViPNet IDS являться туннелируемым ресурсом? 8. Обязаны ли субъекты КИИ оказывать содействие должностным лицам ФСБ России в обнаружении компьютерных атак? 9. Какой компонент не входит в состав ПАК ViPNet IDS? 10. Дайте определение КИИ. |

**8.2.**  **описание показателей и критериев оценивания, шкалы оценивания:** курс считается успешно пройденным, если при прохождении итогового тестирования слушателем набрано не менее 75% правильных ответов на вопросы теста.

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

**8.4.**  **тесты и обучающие задачи (кейсы), иные практикоориентированные формы заданий:** в курсе предусмотрено выполнение 8 практикумов, описание которых представлено в разделе 7.

**8.5.**  **описание процедуры оценивания результатов обучения**: процедуры оценивания итоговых результатов обучения проходит в форме тестирования. Тестирование проходит в онлайн-формате в личном кабинете слушателя в последний день обучения. Доступ к тестированию открывается после успешного прохождения учебного материала курса.

**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** | Васильев Николай Петрович | старший преподаватель НОЧУ ДПО ЦПК «Учебный центр ИнфоТеКС», к.т.н. |  |  | **+** |
| **2** | Попов Алексей Васильевич | старший преподаватель НОЧУ ДПО ЦПК «Учебный центр ИнфоТеКС», к.в.н. |  |  | **+** |
| **3** | Фефилов Александр Валерьевич | преподаватель НОЧУ ДПО ЦПК «Учебный центр ИнфоТеКС», |  |  | **+** |

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

|  |  |
| --- | --- |
| **Учебно-методические материалы** | |
| Методы, формы и технологии | Методические разработки,  материалы курса, учебная литература |
| 1. Занятия проводятся очно в форме онлайн подключения через систему mind.ru  2. Практические работы выполняются на виртуальных образах ПО и ПАК  3. Итоговая аттестация проводится в форме тестирования. Ссылки на тест открываются в личных кабинетах слушателей в последний день обучения. | Учебно-методические материалы расположены в системе дистанционного обучения на сайте https://infotecs-edu.ru/ |

|  |  |
| --- | --- |
| **Информационное сопровождение** | |
| Электронные  образовательные ресурсы | Электронные  информационные ресурсы |
| 1. Сайт Федеральной Службы Безопасности. https://fstec.ru/ 2. ФСТЭК России http://www.fsb.ru/ 3. https://securelist.ru/enciklopediya Энциклопедия информационной безопасности. 4. <https://lib.itsec.ru/articles2/allpubliks> Портал «Информационная безопасность»: новости, публикации, инновации 5. http://internetsecure.ru/ InternetSecure.ru — безопасность в интернет — набор технологий и программ для работы в сети и с компьютером 6. http://laste.arvutikaitse.ee/rus/html/etusiv u.htm Основы безопасности в Интернете для молодежи интерактивный курс по Интерент-безопасности 7. http://www.itn.ru/communities.aspx?cat\_no=71586&t mpl=com 4 этапа защиты компьютера — советы от компании Microsoft. Обеспечение информационной безопасности в учебных заведениях 8. http://www.symantec.com/ru/ru/norton/cl ubsymantec/library/article.jsp?aid=cs\_tea ch\_kids Вопросы безопасности — сайт от компании Symantec 9. http://www.microsoft.com/rus/protect/de fault.mspx# Вопросы обеспечения информационной безопасности от компании Microsoft   http://saferunet.ru/ Центр Безопасного Интернета в России посвящен проблеме безопасной, корректной и комфортной работы в Интернете. Вопросы Интернет-угроз, технологий, способов эффективного противодействия им в отношении пользователей | 1. http://www.securityportal.ru/ Security Portal .RU — сведения по защите информации, защите приватности, безопасным сетевым взаимодействиям, криптографии. 2. http://www.anti-malware.ru/ Anti-Malware.ru — независимый информационно-аналитический портал по безопасности 3. http://www.securitylab.ru/software/1423/ Каталог программ «Защита детей от интернетугроз» (описание, сравнение, оценки). 4. http://download.live.com/familysafety Семейная безопасность — Windows Live - программа от компании Microsoft 5. http://www.etika.ru/ Этика — сайт создан специально для пользователей Рунета, которые хотят работать в этичной, корректной и безопасной среде и готовы участвовать в создании такой среды 6. http://ru.wikipedia.org/wiki/Netiquette Сетевой этикет — Википедия 7. http://www.antispam.ru/ Проект Антиспам.Ру 8. http://www.citforum.ru/security/ CITFORUM — информационная безопасность (большое количество материалов по теме) 9. http://www.comp-doctor.ru/ Компьютер и здоровье: болезни от компьютера, профилактика и лечение. Здоровый образ жизни и профессиональные заболевания пользователей компьютеров. Как выбрать безопасные для здоровья компьютер и программы, правильно организовать рабочее место 10. http://www.saferinternet.ru/ Безопасный интернет - специальный портал, созданный по вопросам безопасного использования сети Интернет. Документы, материалы и многое другое 11. http://saferinternet.ru/ Портал Российского Оргкомитета по проведению Года Безопасного Интернета (ресурсы, ссылки, документы, материалы по проблематике) 12. http://www.infoforum.ru/ Национальный форум информационной безопасности "ИНФОФОРУМ" — электронное периодическое издание по вопросам информационной безопасности 13. Security Lab | http://www.securitylab.ru/ 14. **Anti-Malware |**https://www.anti-malware.ru/ Информационно-аналитический центр, посвященный информационной безопасности. |

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

|  |  |
| --- | --- |
| Вид занятий | Наименование оборудования,  программного обеспечения |
| Лекция | Вебинарная платформа mind.com |
| Практикум | 1. Среда виртуализации Oracle VM VirtualBox 5.3.x 2. Виртуальные машины – образы программно-аппаратных комплексов ViPNet 3. Программное обеспечение ViPNet Administrator, ViPNet Coordinator Linux, ViPNet Client, ViPNet Policy Manager, ViPNet IDS 4. Программный комплекс «Ampire» 5. Лицензии на учебные сети ViPNet |

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

ПАСПОРТ КОМПЕТЕНЦИИ

Кибербезопасность и защита корпоративных сетей

Негосударственное образовательное частное учреждение

дополнительного профессионального образования

центр повышения квалификации «Учебный центр «ИнфоТеКС»

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Наименование компетенции | | Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации | |
| 2. | Указание типа компетенции | общекультурная/  универсальная |  | |
| общепрофессиональ ная |  | |
| профессиональная | + | |
| профессионально-специализированная |  | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | |  | |
| 4. | Дескриптор знаний, умений и навыков по уровням | | Уровни сформирован ности 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.) | Способен установить ПО ViPNet Administrator, ViPNet Coordinator, ViPNet Client. Навыки настройки ПО слабые: встречаются ошибки при формировании справочной и ключевой информации сети; может отсутствовать связность между узлами защищенной сети. |
|  | | Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределён ности, сложности.) | Способен установить ПО ViPNet Administrator, ViPNet Coordinator, ViPNet Client, настраивать параметры защищённых сетей различной топологии, настраивает взамодействие между узлами защищенной сети согласно данной схеме. |
|  | | Продвинутый  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Способен установить ПО ViPNet Administrator, ViPNet Coordinator, ViPNet Client, настраивать параметры защищённых сетей различной топологии, настраивает взаимодействие между узлами защищенной сети согласно данной схеме.  Способен выполнять модификацию защищенной сети, настраивать межсетевое взаимодействие, наделять пользователей различными полномочиями; устранять неполадки в работе защищённой сети как на рабочих местах клиентов, так и централизованно в программе ViPNet Administrator. |
|  | | 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.) | Способен установить ПО ViPNet Administrator, ViPNet Coordinator, ViPNet Client, настраивать параметры защищённых сетей различной топологии, настраивает взаимодействие между узлами защищенной сети согласно данной схеме.  Способен выполнять модификацию защищенной сети, настраивать межсетевое взаимодействие, наделять пользователей различными полномочиями; устранять неполадки в работе защищённой сети как на рабочих местах клиентов, так и централизованно в программе ViPNet Administrator.  Способен вносить предложения по усовершенствованию топологии защищенной сети, настраивает политику безопасности в ПО ViPNet Policy Manager, централизованно управляет защищенной сетью. |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | Необходимо владеть компетенцией цифровой грамотности | |
| 6. | Средства и технологии оценки | | Знает:   * принципы работы защищенных виртуальных сетей; * принципы действия, технологию использования и методику применения защищенных сетей; * методы организации защищенных сетей ViPNet   Умеет:   * организовывать доступ к защищаемым ресурсам и наделять полномочиями пользователей (в соответствии с решением по доступу пользователей к информационным ресурсам и в объеме, соответствующем этому решению);   Владеет:   * методами управления защищенными сетями; * технологией организации VPN; * методикой использования системы защиты информации ViPNet | |
| 7. | Наименование компетенции | | Способность принимать участие в формировании комплекса мер по обеспечению информационной безопасности, разрабатывать предложения по совершенствованию системы управления информационной безопасностью | |
| 8. | Указание типа компетенции | общекультурная/  универсальная |  | |
| общепрофессиональ ная |  | |
| профессиональная | + | |
| профессионально-специализированная |  | |
| 9. | Определение, содержание и основные сущностные характеристики компетенции | |  | |
| 10. | Дескриптор знаний, умений и навыков по уровням | | Уровни сформирован ности 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.) | Способен в составе группы мониторинга обнаружить вторжение на платформе ПК «Ampire».  Не всегда способен определить вектор атаки. Не всегда способен дать рекомендации по реагированию на атаку. |
|  | | Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределён ности, сложности.) | Способен в составе группы мониторинга обнаружить вторжение на платформе ПК «Ampire», правильно определяет вектор атаки на информационную систему, дает правильные рекомендации по поиску уязвимости в системе.  В составе группы реагирования верно находит уязвимость и закрывает ее. |
|  | | Продвинутый  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Способен в составе группы мониторинга обнаружить вторжение на платформе ПК «Ampire», правильно определяет вектор атаки на информационную систему, дает правильные рекомендации по поиску уязвимости в системе.  В составе группы реагирования верно находит уязвимость и закрывает ее.  Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью. Способен быстро определить вектор атаки и закрыть уязвимости наиболее рациональным методом. |
|  | | 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.) | Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью. Способен быстро определить вектор атаки и закрыть уязвимости наиболее рациональным методом.  Способен настраивать средства защиты информации в организации на блокирование различных атак извне. |
| 11. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | Необходимо владеть компетенцией цифровой грамотности, компетенцией системного администрирования | |
| 12. | Средства и технологии оценки | | Знает:   * + принципы работы программно-аппаратного комплекса ViPNet IDS;   + порядок создания защищенного канала между взаимодействующими объектами через систему общего пользования с использованием линейки продуктов СЗИ ViPNet;   + подсистемы обнаружения атак, подсистемы защиты от преднамеренных воздействий, контроля целостности информации;   + принципы действия, технологию использования и методику применения программно-аппаратного комплекса ViPNet IDS;   + методы мониторинга и анализа событий и инцидентов информационной безопасности   Умеет:   * организовывать доступ к программно-аппаратным комплексам ViPNet IDS и наделять полномочиями пользователей (в соответствии с решением по доступу пользователей к программно-аппаратным комплексам в объеме, соответствующем этому решению); * проводить аудит журналов на предмет попыток НСД и прочих нарушений; * осуществлять контроль правильности функционирования программно-аппаратного комплекса ViPNet IDS; * проводить мониторинг и анализ событий и инцидентов информационной безопасности.   Владеет:   * методами управления программно-аппаратным комплексом ViPNet IDS; * технологией мониторинга и анализа событий и инцидентов информационной безопасности; * методами и средствами выявления угроз безопасности информации, методиками выявления каналов утечки информации; * оценкой эффективности предлагаемых и реализуемых организационно-технических решений по обеспечению безопасности информации; * навыками по устранению уязвимостей в информационных системах общего и специального назначения | |

**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**: приложены

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

Повышение квалификации в целях осуществления своей профессиональной деятельности, получение новых знаний по компетенции.

**VII.Дополнительная информация**

**VIII.Приложенные Скан-копии**

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