|  |  |
| --- | --- |
| C:\Users\T'rain\Desktop\логотип 2016 УКРТБдля документов.jpg | МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ БАШКОРТОСТАН  Государственное бюджетное профессиональное образовательное учреждение  Уфимский колледж радиоэлектроники, телекоммуникаций и безопасности |

|  |  |
| --- | --- |
| СОГЛАСОВАНО  Председатель ГАК  \_\_\_\_\_\_\_\_\_\_\_\_ А.А. Климов  «26» ноября 2021 г. | УТВЕРЖДАЮ  Директор ГБПОУ УКРТБ  \_\_\_\_\_\_\_\_\_\_\_\_ И.В. Нуйкин  «26» ноября 2021 г. |

**ПРОГРАММА ГОСУДАРСТВЕННОЙ (ИТОГОВОЙ) АТТЕСТАЦИИ ВЫПУСКНИКОВ УКРТБ  
ПО СПЕЦИАЛЬНОСТИ СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ**

|  |  |  |  |
| --- | --- | --- | --- |
| 11.02.15 |  | Инфокоммуникационные сети и системы связи | |
| *код* |  | *наименование специальности* | |
| Квалификация: | | | Специалист по обслуживанию телекоммуникаций |
|  |  | *наименование квалификации* | |

|  |  |
| --- | --- |
|  | СОГЛАСОВАНО  Зам. директора ГБПОУ УКРТБ  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Л.Р. Туктарова  Зав. кафедрой телекоммуникаций  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Э.Р. Кабирова |

Уфа 2021 год

**Содержание**

|  |  |
| --- | --- |
| 1. Общие положения |  |
| 2. Процедура проведения государственной итоговой аттестации |  |
| 3. Требования к выпускной квалификационной работе |  |
| 4. Оценка результатов государственной итоговой аттестации |  |
| 5. Порядок апелляции и пересдачи государственной  итоговой аттестации |  |
| Приложение 1. Примерный план работы центра проведения демонстрационного экзамена |  |
| Приложение 2. Примерная тематика выпускных квалификационных работ |  |
| Приложение 3. Примерное задание для демонстрационного экзамена |  |

**1. ОБЩИЕ ПОЛОЖЕНИЯ**

**1.1. Область применения программы ГИА**

Программа государственной итоговой аттестации (далее – ГИА) является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности

|  |  |  |
| --- | --- | --- |
| 11.02.15 |  | Инфокоммуникационные сети и системы связи |
| *код* |  | *наименование специальности* |

утвержденного Приказом Министерства образования и науки 9 декабря 2016 года № 1584 (зарегистрирован Министерством юстиции Российской Федерации 26 декабря 2016г., регистрационный №44945).

Квалификация выпускника: специалист по обслуживанию телекоммуникаций.

Образовательная программа реализуется на базе основного общего образования.

**1.2. Цели и задачи государственной итоговой аттестации**

Целью государственной итоговой аттестации является установление соответствия уровня освоенности компетенций, обеспечивающих соответствующую квалификацию и уровень образования обучающихся, Федеральному государственному образовательному стандарту среднего профессионального образования. ГИА призвана способствовать систематизации и закреплению знаний и умений обучающегося по специальности при решении конкретных профессиональных задач, определить уровень подготовки выпускника к самостоятельной работе.

**1.3. Нормативные правовые документы и локальные акты, регулирующие вопросы организации и проведения ГИА**

1. Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

2. Федеральный государственный стандарт среднего профессионального образования по специальности 11.02.15 Инфокоммуникационные сети и системы связи, Приказом Министерства образования и науки 9 декабря 2016 года № 1584 (зарегистрирован Министерством юстиции Российской Федерации 26 декабря 2016г., регистрационный №44945).

3. Приказ Министерства образования и науки Российской Федерации от 14 июня 2013 г. №464 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования»;

4. Приказ Министерства образования и науки Российской Федерации от 16 августа 2013 г. №968 «Об утверждении Порядка проведения государственной итоговой аттестации по образовательным программам среднего профессионального образования» с изменениями, внесенными приказами Министерства образования и науки Российской Федерации от 31 января 2017 г. №74 и от 17 ноября 2017 г. № 1138;

5. Приказ Министерства образования и науки Российской Федерации от 29 октября 2013 г. №1199 «Об утверждении перечней профессий и специальностей среднего профессионального образования»;

6. Положение о проведении демонстрационного экзамена в рамках ГИА.

**1.4 Формы проведения государственной итоговой аттестации**

Государственная итоговая аттестация в соответствии с ФГОС СПО проводится в форме защиты выпускной квалификационной работы, которая выполняется в виде дипломной работы (дипломного проекта) и демонстрационного экзамена.

**1.5 Требования к уровню подготовки выпускника по профессиональной образовательной программе в соответствии с ФГОС СПО**

**Требования к уровню подготовки выпускника к защите выпускной квалификационной работы по программе подготовки специалиста среднего звена.**

1.5.1 Иметь практический опыт в:

* выполнении монтажа и настройке сетей проводного беспроводного абонентского доступа в соответствии с действующими отраслевыми стандартами;
* осуществлении технического обслуживания кабелей связи и оконечных структурированных кабельных устройств в соответствии с действующими отраслевыми стандартами;
* выполнении монтажа, инсталляции компьютерных сетей в соответствии с действующими отраслевыми стандартами;
* администрировании сетевого оборудования в соответствии с действующими отраслевыми стандартами;
* выполнении монтажа, первичной инсталляции, настройке системы видеонаблюдения и безопасности в соответствии с действующими отраслевыми стандартами.
* выполнении монтажа, демонтажа, первичной инсталляции, мониторинге, диагностике инфокоммуникационных систем передачи в соответствии с действующими отраслевыми стандартами.
* устранении аварий и повреждений оборудования инфокоммуникационных систем;
* разработке проектов инфокоммуникационных сетей и систем связи для предприятий и компаний малого и среднего бизнеса.
* анализе сетевой инфраструктуры;
* выявлении угроз и уязвимости в сетевой инфраструктуре;
* разработке комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи;
* осуществлении текущего администрирования для защиты инфокоммуникационных сетей и систем связи;
* использовании специализированного программного обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи.
* планировании производства в рамках структурного подразделения организации на основе знания психологии личности и коллектива;
* организации производственной деятельности в рамках структурного подразделения организации;
* приемах руководства производственной деятельностью структурного подразделения, отвечающего за предоставление телематических услуг.
* адаптации, монтаже, установке и настройке конвергентных инфокоммуникационных систем в соответствии с действующими отраслевыми стандартами;
* администрировании конвергентных систем в соответствии с рекомендациями Международного союза электросвязи.

1.5.2 Уметь

* разрабатывать проект мультисервисной сети доступа с предоставлением услуг связи;
* проектировать структурированные медные и волоконно-оптические кабельные сети, сети для видеонаблюдения и систем безопасности объекта;
* читать, интерпретировать и анализировать техническую спецификацию и чертежи проекта;
* составлять альтернативные сценарии модернизации сетей доступа, способных поддерживать мультисервисное обслуживание;
* выполнять монтаж и демонтаж кабельных трасс и прокладку кабелей для систем видеонаблюдения, систем безопасности объекта; охранно-пожарной сигнализации, систем пожаротушения, контроля доступа;
* подготавливать волоконно-оптический кабель к монтажу, сращиванию различными способами;
* выполнять документирование кабельной проводки: марки кабелей, маркировку участков кабеля, телекоммутационных шкафов, стоек, панелей и гнезд, жил, модулей в кроссе, шкафах, муфте;
* осуществлять установку оборудования и программного обеспечения, первичную инсталляцию, настройку, диагностику и мониторинг работоспособности оборудования широкополосного проводного и беспроводного абонентского доступа;
* осуществлять организацию электронного документооборота в соответствии с потребностями заказчика;
* осуществлять техническое обслуживание оборудования сетей мультисервисного доступа; оформлять техническую документацию,
* осуществлять разработку проектов коммутационных станций, узлов и сетей электросвязи для предприятий и компаний малого и среднего бизнеса;
* составлять сценарии возможного развития телекоммуникационной сети и ее фрагментов; читать техническую документацию;
* осуществлять первичную инсталляцию программного обеспечения инфокоммуникационных систем;
* осуществлять организацию эксплуатации и технического обслуживания инфокоммуникационных систем на основе концепции Telecommunication management network;
* производить настройку и техническое обслуживание, выполнять диагностику цифровых систем коммутации и систем передачи.
* классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;
* определять оптимальные способы обеспечения информационной безопасности;
* осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;
* выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов
* выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;
* защищать базы данных при помощи специализированных программных продуктов.
* разрабатывать положение о структурном подразделении, штатное расписание и должностные инструкции;
* планировать бюджет структурного подразделения; рационально организовывать рабочие места, рассчитывать нормы времени и норму выработки;
* рассчитывать и оценивать показатели, характеризующие эффективность организации обслуживания;
* мотивировать работников на решение производственных задач;
* предотвращать возникновения конфликтных ситуаций;
* осуществлять подбор необходимых материально-технических ресурсов на основе анализа по ценам и другим рыночным показателям;
* рассчитывать технико-экономические показатели; составлять бизнес-план,
* интегрировать сетевое телекоммуникационное оборудование с использованием протоколов цифровой сигнализации EUROISDN, DSS1 (EDSS), SS7, QSIG;
* выполнять монтаж и настройку конвергентных систем связи и сетевого оборудования различных вендоров;
* администрировать телекоммуникационные системы и конвергентные сети связи с помощью локальных пакетов прикладных программ, унифицировать стационарные и сотовые разновидности инфокоммуникационных услуг путем интеграции приложений, написанных в различных операционных системах для мобильных устройств;
* обслуживать абонентские устройства с доступом в сеть Интернет на основе программных оболочек и унифицированных приложений.

1.5.3 Знать

* современные технологии, используемые для развития проводных и беспроводных сетей доступа;
* принципы построения сетей мультисервисного доступа; базовые технологии;
* различные виды кабелей, классификацию, конструктивные особенности, их технические характеристики, технологические особенности строительства направляющих систем электросвязи при прокладке кабелей связи в кабельной канализации, в грунте, подвеске на опорах;
* правила прокладки медных кабельных линий и волоконно-оптических кабелей в зданиях и помещениях пользователя;
* требования к телекоммуникационным помещениям;
* назначение, принципы построения, область применения горизонтальной и магистральной подсистем структурированных кабельных систем;
* требования, предъявляемые при прокладке и монтаже волоконно-оптических линиях связи (далее - ВОЛС);
* методику монтажа и демонтажа магистральных оптических кабелей, муфт;
* назначение, практическое применение, конструкцию и принципы работы измерительных приборов и тестового оборудования;
* организацию измерений при монтаже и сдаче в эксплуатацию в эксплуатацию ВОЛС: контрольных и приемно-сдаточных испытаний на линиях связи;
* работу сетевых протоколов в сетях мультисервисных сетях доступа;
* принципы проектирования и построения систем видеонаблюдения и безопасности.
* методы коммутации и их использование в сетевых технологиях;
* архитектуру и принципы построения сетей с коммутацией каналов;
* принципы пакетной передачи, функциональную модель инфокоммуникационной сети с коммутацией пакетов NGN, оборудование сетей передачи данных с пакетной коммутацией;
* технологию MPLS: архитектуру сети, принцип работы;
* принципы проектирования, построения аппаратуры оптических систем передачи и транспортных сетей с временным мультиплексированием TDM и волновым мультиплексированием WDM;
* модели оптических транспортных сетей: SDH, ATM, OTN-ОТН, Ethernet;
* технологии мультиплексирования и передачи в транспортных сетях.
* принципы построения информационно-коммуникационных сетей;
* международные стандарты информационной безопасности;
* акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия;
* технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;
* классификацию угроз сетевой безопасности;
* методы и способы защиты информации, передаваемой по кабельным направляющим системам;
* правила проведения возможных проверок согласно нормативным документам Федеральной службы по техническому и экспортному контролю;
* средства защиты различных операционных систем и среды передачи информации.
* Законодательство Российской Федерации в области организации труда и предпринимательской деятельности;
* Законодательство Российской Федерации в области предоставления качественных услуг потребителям;
* современное состояние и перспективы развития телекоммуникационного сектора Российской Федерации; сущность, значение и направления деятельности организации;
* порядок расчета бюджета структурных подразделений организации, отвечающих за предоставление телематических услуг;
* структуру организации, организацию рабочих мест и условий труда;
* систему показателей и нормативов качества обслуживания и качества услуг связи;
* методы конструктивного разрешения конфликтов; элементы PR-технологий при продвижении услуг связи конкретным потребителям.
* современные методы и средства управления телекоммуникационными системами и конвергентными сетями связи;
* технические составляющие интегрированной транспортной сети CoreNetwork;
* платформы предоставления инфокоммуникационных услуг с возможностями множественного доступа;
* способы реализации принципа конвергенции в телекоммуникационных услугах на основе концепции All-IP и с использованием программных оболочек логических сетей (IP).

**2. ПРОЦЕДУРА ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ**

**2.1. Проведение демонстрационного экзамена**

2.1.1 Выбор оценочной документации для демонстрационного экзамена

Демонстрационный экзамен предусматривает моделирование реальных производственных условий для решения практических задач профессиональной деятельности в соответствии с лучшими мировыми и национальными практиками.

Для проведения демонстрационного экзамена по специальности 11.02.15 Инфокоммуникационные сети и системы связи выбраны компетенции   
02 Информационные кабельные сети Выбраны комплект оценочной документации (КОД) №1.4, F7 Корпоративная защита от внутренних угроз информационной безопасности, выбран комплект оценочной документации (КОД) №1.1.

2.1.2 Сроки и место проведения демонстрационного экзамена

Объем времени и сроки, отводимые на подготовку к демонстрационному экзамену: 2 недели, май.

Сроки проведения демонстрационного экзамена: 2 дня, июнь.

Место проведения демонстрационного экзамена – Центр проведения демонстрационных экзаменов по адресу: г. Уфа, ул. Генерала Горбатова, 11.

13.06.2022-26.06.2022 г. в том числе ДЭ 09.06.2022-10.06.2022 г.

Форма участия: индивидуальная.

КОД №1.4 по Информационным кабельным сетям рассчитан на выполнение заданий продолжительностью 6 часов.

КОД №1.1 по Корпоративная защита от внутренних угроз информационной безопасности рассчитан на выполнение заданий продолжительностью 6,5 часов.

Примерные планы работы Центра проведения демонстрационного экзамена по КОД №1.4 по компетенции Информационные кабельные сети приведены в приложении 1а.

Примерные планы работы Центра проведения демонстрационного экзамена по КОД №1.1 приведены в приложении 1б

2.1.3.1 Перечень знаний, умений и навыков в соответствии со Спецификацией стандарта компетенции 02 Информационные кабельные сети (WorldSkills Standards Specifications, WSSS), проверяемый в рамках комплекта оценочной документации.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Номер раздела**  **WSSS** | **Наименование раздела WSSS** | | **Содержание раздела WSSS:**  **Специалист должен знать** | **Важность раздела**  **WSSS (%)** |
| **1** | **2** | | **3** | **4** |
| 1 | Организация работ | | Специалист должен знать и понимать:Законодательство в области охраны труда;Правила оказания первой медицинской  помощи;Последствия влияния неустойчивой и ненадёжной сетевой инфраструктуры на бизнес-процессы организации;Правила работ с лазерными установками;Назначение, правила безопасного  использования, обслуживания и хранения оборудования;Важность обеспечения безопасности при работе с пользовательскими  данными;Важность правильной утилизации и переработки  отходов;Значимость концентрации внимания к деталями выполнении всех видов работ;Важность методичности выполнения работ;Важность разработки новых методов и техник;Значимость собственного  профессионального роста;Технологии бережливого  производства;Способы организации защитного заземления.Специалист должен уметь:Следовать правилам и стандартам  безопасности;Поддерживать безопасную рабочую обстановку, включая использование лестниц для выполнения работ на высоте;Использовать индивидуальные средства защиты;Подбирать и использовать средства защиты от электростатического разряда;Безопасно подбирать,  использовать, чистить и хранить инструмент и  оборудование;Организовывать рабочее место для максимальной эффективности производства работ и поддержания  чистоты;Осуществлять комплекс мер по организации защитного заземления;Планировать и перепланировать задачи в соответствии с меняющимися приоритетами;Работать максимально эффективно,  соблюдать отраслевые стандарты, контролировать и проверять результаты работы;Постоянно заниматься профессиональным  развитием, изучать и знать отраслевые стандарты, контролировать | 1,7 |
|  |  | обновление стандартов;Проявлять энтузиазм в апробации новых  методов и методик. | |  | |
| 2 | Коммуникативные навыки | Специалист должен знать и понимать:Важность умения слушать как части эффективного общения;Роли и запросы коллег и наиболее  эффективные методы общения;Важность построения и поддержания продуктивных рабочих взаимоотношений с  коллегамиуправляющими;Техники эффективной командной работы;Техники разрешения недопонимания и конфликтных  ситуаций;Процесс управления гневом и стрессом для разрешения конфликтных ситуаций.Специалист должен уметь:Демонстрировать сильные навыки слушания и задавания вопросов для более глубокого  понимания сложных ситуаций;Последовательно и эффективно общаться с коллегами в устной и письменной форме;Распознавать и  адаптироваться к изменяющимся нуждам коллег;Активно участвовать в создании сильной и эффективной команды;Делиться знаниями и опытом с коллегами и развивать благоприятную культуру обучения;Справляться с чужими напряженностью и гневом, обеспечивая уверенность в том, что проблемы могут быть решены;Обсуждать требования заказчиков и обеспечивать Экспертные советы и консультации;Взаимодействовать с другими профессионалами поставщиками для формирования полностью индивидуального пакета, который удовлетворяет потребностям  заказчика;Понимать, что выполнение работ в сетевойинфраструктуре влияет на нагруженное работающее оборудование, демонстрировать внимательность и осторожность, сводить ущерб к  минимальному;Заранее планировать предстоящие работы своевременно уведомлять заказчиков;Успешно отстаивать свои интересы;Убедительно аргументировать свою позицию;Производить хорошее впечатление на  собеседников | | 0,40 | |
| 3 | Планирование и проектирование | Специалист должен знать и понимать:Правила построения  структурированных кабельных систем;Организацию сетей FTTх,  GPON;Этапы производства работ по проектированию и монтажу  кабельных систем;Построение беспроводных сетей(Wi-Fi);Построение сетей кабельного телевидения(CCTV), систем безопасности и домашней автоматизации;Виды сетевого оборудования и алгоритмы  настройки;Применение технологий «Умный дом»;Терминологию и УГО,  используемые в отраслевых спецификациях и чертежах;Состав | | 1,40 | |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | исполнительной документации и порядок сдачи объектов связи в эксплуатацию;Методы планирования, составления расписаний и  расстановки приоритетов;Методы обеспечения сетевой безопасности и защиты от атак;Методику расчета производительности сети;Математику и физику;Электронику и электротехнику.Специалист должен  уметь:Заполнять техническую документацию;Решать практические задачи;Работать самостоятельно, планировать, упорядочивать работу, расставлять приоритеты с целью обеспечения максимальной  эффективности и придерживаться запланированных временных интервалов;Планировать работу для получения заданных  результатов;Готовить, читать, интерпретировать и анализировать  чертежи и спецификации;Выбирать инструмент, наиболее подходящий для планируемых задач;Выбирать кабели в зависимости от их  назначения;Оценивать и предотвращать риски;Планировать  распределение кабелей для минимизации ущерба и эстетичности укладки;Применять математические навыки для планирования,  подготовки и выполнения задач по укладке кабеля;Читать, понимать и применять инструкции производителей;Интерпретировать и  анализировать сложные планы и спецификации;Планировать IP- сети;Создавать чертежи в специализированном ПО;Составлять  спецификации оборудования и расходных материалов. |  |
| 4 | Укладка кабеля | Специалист должен знать и понимать:Различные типы кабеля,  характеристики, область применения и его влияние на другие аспекты сети.Методы эффективной укладки кабеля в кабельные  каналы;Стандарты по маркировке пучков кабелей и кабелей;Важность соблюдения радиусов изгиба при укладке кабеля;Способы крепления пучков кабеля в кабельных лотках;Важность планирования запасов  кабеля и их укладки.Специалист должен уметь:Производить монтаж  кабельных систем в соответствии со стандартами;Качественно и быстро укладывать кабели в кабельные каналы и иные конструктивы, в том  числе с применением специализированных технических  средств;Расставлять приоритеты, укладываться в отведённые сроки при выполнении работ;Производить маркировку;Соблюдать чистоту на  рабочем месте при производстве монтажных работ. | 8,80 |
| 6 | Структурированные кабельные  системы | Специалист должен знать и понимать:  Правила построения СКС; | 19,90 |
|  |  | Виды и характеристики медно-жильных кабелей; Правила маркировки;  Правила укладки кабеля; Способы тестирования. Специалист должен уметь:  Производить сборку телекоммуникационных стоек и шкафов; Производить монтаж патч-панелей, телекоммуникационных розеток; Устанавливать и подключать активное сетевое оборудование; Производить тестирование и анализировать результаты;  Производить маркировку;  Производить формирование и укладку пучков кабеля. |  |
| 7 | Технологии "Умный дом" | Специалист должен знать и понимать:СтандартыIEEE802.11;Назначение и применение технологий «умный дом» в повседневной жизни;Виды,  характеристики, алгоритмы настройкиактивного сетевого оборудования (IP камеры, IP телефоны, маршрутизаторы, коммутаторы, WI-FI  беспроводные точки доступа, сетевой принтер, ноутбук, Smart TV, CATV, IP-TV приставка, IP-домофон, IP-PBX);Системы домашней и промышленной автоматизации и обеспечения безопасности (контроллеры, датчики, сенсоры и исполнительные  устройства);Принципы IoT (Интернет вещей) и IIoT (Промышленный Интернет вещей).Специалист должен уметь:Производить базовую  настройку активного сетевого оборудования;Настраивать беспроводные системы связи;Производить монтаж оборудования и устанавливать  современные и востребованные решения типа «умный  дом»;Устанавливать и настраивать мобильные приложения для мониторинга и управления домашней  автоматизацией;Администрировать виртуальные IP-PBX;Работать с  анализаторами беспроводных сетей;Настраивать системы IoT и IIoT. | 5,80 |
| 9 | Измерения | Специалист должен знать и понимать:  Принципы и назначение измерительных устройств; Практическое применение измерительных устройств. Специалист должен уметь:  Инспектировать и чистить разъёмные соединения и исправлять при необходимости;  Производить измерения характеристик волоконно- оптических кабелей  при помощи тестеров оптических потерь (OTLS) и оптических  рефлектометров(OTDR);  Подбирать необходимое оборудование для тестирования; Заполнять протоколы измерений. | 3,20 |

2.1.3.2 Перечень знаний, умений и навыков в соответствии со Спецификацией стандарта компетенции F7 Корпоративная защита от внутренних угроз информационной безопасности (WorldSkills Standards Specifications, WSSS), проверяемый в рамках комплекта оценочной документации.

|  |  |  |
| --- | --- | --- |
| Раздел WSSS | Наименование раздела WSSS | Важность (%) |
| 1 | **Организация работы и управление**  Специалист должен знать и понимать:  - понимание принципов работы специалиста по информационной безопасности и их применение;  - знание принципов и положений безопасной работы в общем и по отношению к корпоративной среде;  - регламентирующие документы в области безопасности информационных систем;  - регламентирующие документы в области охраны труда и безопасности жизнедеятельности;  - важность организации труда в соответствии с методиками;  - методы и технологии исследования;  -важность управления собственным профессиональным развитием;  -скорость изменения ИТ-сферы и области информационной безопасности, а также важность соответствия современному уровню.  -важность умения слушать собеседника как части эффективной коммуникации;  -роли и требования коллег и наиболее эффективные методы коммуникации;  -важность построения и поддержания продуктивных рабочих отношений с коллегами и управляющими;  -способы разрешения непонимания и конфликтующих требований;  -методы управления стрессом и гневом для разрешения сложных ситуаций.  Специалист должен уметь:  - поддерживать безопасную, аккуратную и эффективную рабочую зону;  -использовать все оборудование и программное обеспечение безопасно и в соответствии с инструкциями производителя;  -следовать предписаниям в области охраны труда и безопасности жизнедеятельности;  -регулярно планировать свою работу и корректировать планы в соответствии с изменяющимися приоритетами;  -поддерживать рабочее место в должном состоянии и порядке.  -демонстрировать развитые способности слушать и задавать вопросы для более глубокого понимания сложных ситуаций;  -выстраивать эффективное письменное и устное общение;  -понимать изменяющиеся требования и адаптироваться к ним. | 3 |
| 2 | **Установка, конфигурирование и устранение неисправностей**  Специалист должен знать и понимать:  - сетевое окружение;  -сетевые протоколы;  -знать методы выявления и построения путей движения информации в организации;  -подходы к построению сети и как сетевые устройства могут быть настроены для эффективного взаимодействия;  -типы сетевых устройств;  -разнообразие операционных систем, их возможности с точки зрения использования пользователями и для развёртывания компонент систем защиты от внутренних угроз;  -процесс выбора подходящих драйверов и программного обеспечения для разных типов аппаратных средств и операционных систем;  -важность следования инструкциям и последствия, цену пренебрежения ими;  - меры предосторожности, рекомендуемые к принятию перед установкой ПО или обновлением системы;  -этапы установки системы корпоративной защиты от внутренних угроз;  -знать отличия различных версий систем корпоративной защиты от внутренних угроз;  -знать какие СУБД поддерживаются системой;  -знать назначение различных компонент версий систем корпоративной защиты от внутренних угроз;  -знать технологии программной и аппаратной виртуализации;  -знать особенности работы основных гипервизоров (мониторов виртуальных машин), таких как VirtualBox, VMWareWorkstation;  -цель документирования процессов обновления и установки.  -важность спокойного и сфокусированного подхода к решению проблемы;  -значимость систем ИТ-безопасности и зависимость пользователей и организаций от их доступности;  -популярные аппаратные и программные ошибки;  -знать разделы системы корпоративной безопасности, которые обычно использует системный администратор;  -аналитический и диагностический подходы к решению проблем;  -границы собственных знаний, навыков и полномочий;  -ситуации, требующие вмешательства службы поддержки;  -стандартное время решения наиболее популярных проблем.  Специалист должен уметь:  - интерпретировать пользовательские запросы и требования с точки зрения корпоративных требований;  -применять все типы конфигураций, программные и аппаратные обновления на все типы сетевых устройств, которые могут быть в сетевом окружении;  -настраивать сетевые устройства;  -администрирование автоматизированных технические средства управления и контроля информации и информационных потоков;  -навыки системного администрирования в операционных системах WindowsServer и LinuxRedHatEnterpriseLinux;  -установка серверной части системы корпоративной защиты от внутренних угроз;  -установка СУБД различного вида;  -установка агентской части системы корпоративной защиты от внутренних угроз;  -запуск гостевых виртуальных машин и практическая работа с ними с использованием современных гипервизоров;  -настройка отдельных компонент системы корпоративной защиты от внутренних угроз и системы в целом;  -использовать дополнительные утилиты если это необходимо;  -уметь проверять работоспособность системы и выявлять неисправности, устранять проблемы и проводить контрольные проверки;  -подходить к проблеме с необходимым уровнем уверенности для успокоения пользователя в случае необходимости;  - уметь сконфигурировать систему, чтобы она получала теневые копии;  -регулярно проверять результаты собственной работы во избежание проблем на последующих этапах;  - демонстрировать уверенность и упорство в решении проблем;  -быстро узнавать и понимать суть неисправностей и разрешать их в ходе самостоятельной управляемой работы, точно описывать проблему и документировать её решение;  -тщательно расследовать и анализировать сложные, комплексные ситуации и проблемы, применять методики поиска неисправностей;  -выбирать и принимать диагностирующее ПО и инструменты для поиска неисправностей; | 15 |
| 4 | **Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз**  Специалист должен знать и понимать:  - технологии работы с политиками информационной безопасности;  - создание новых политик, модификация существующих;  - общие принципы при работе интерфейсом системы защиты корпоративной информации;  - объекты защиты, персоны;  - ключевые технологии анализа трафика;  - типовые протоколы и потоки данных в корпоративной среде, такими как: корпоративная почта (протоколы SMTP, ESMTP, POP3, IMAP4)  - веб-почта;  - интернет-ресурсы: сайты, блоги, форумы и т.д. (протоколы HTTP, HTTPS);  - социальные сети;  - интернет-мессенджеры: OSCAR (ICQ), Telegram, Jabber, XMPP, Mail.ru Агент, GoogleTalk, Skype, QIP;  - принтеры: печать файлов на локальных и сетевых принтерах;  - любые съемные носители и устройства;  - осознание важности полноты построения политик безопасности для выявления всех возможных инцидентов и выявления фактов утечек;  - типы угроз информационной безопасности, типы инцидентов,  - технологий анализа трафика при работе политиками информационной безопасности в системе корпоративной защиты информации;  - основные разделы и особенности работы интерфейса управления системы корпоративной защиты информации;  - алгоритм действий при разработке и использовании политик безопасности, основываясь на различных технологиях анализа данных;  - типовые сигнатуры, используемые для детектирования файлов, циркулирующих в системах хранения и передачи корпоративной информации;  - роль фильтров при анализе перехваченного трафика; Технические ограничения механизма фильтрации, его преимущества и недостатки;  - разделы системы корпоративной безопасности, которые используются офицером безопасности в повседневной работе; -особенности обработки HTTP-запросов и писем, отправляемых с помощью веб-сервисов;  -технологии анализа корпоративного трафика, используемые в системе корпоративной защите информации;  Специалист должен уметь:  - создать в системе максимально полный набор политик безопасности, перекрывающий все возможные каналы передачи данных и возможные инциденты;  - работа с разделом технологии системы корпоративной защиты: категории и термины, текстовые объекты;  - работа с событиями, запросы, объекты перехвата, идентификация контактов в событии;  - работа со сводками, виджетами, сводками;  - работа с персонами;  - работа с объектами защиты;  - провести имитацию процесса утечки конфиденциальной информации в системе;  - создать непротиворечивые политики, соответствующие нормативной базе и законодательству;  - задокументировать созданные политики используя в соответствии с требованиями современных стандартов в области защиты информации.  - работа с категориями и терминами;  - использование регулярных выражений;  - использование морфологического поиска;  - работа с графическими объектами;  - работа с выгрузками и баз данных;  - работа с печатями и бланками;  - работа с файловыми типами;  -эффективно использовать механизмы создания фильтров для анализа перехваченного трафика и выявленных инцидентов; | 20,8 |
| 6 | **Технологии агентского мониторинга**  Специалист должен знать и понимать:  - функции агентского мониторинга;  -общие настройки системы агентского мониторинга;  -соединение с LDAP-сервером и синхронизация с ActiveDirectory;  - политики агентского мониторинга, особенности их настройки;  - особенности настроек событий агентского мониторинга;  - механизмы диагностики агента, подходы к защите агента.  Специалист должен уметь:  - установка и настройка агентского мониторинга;  - создание политик защиты на агентах;  - работа в консоли управления агентом;  - фильтрация событий;  - настройка совместных событий агентского и сетевого мониторинга;  - работа с носителями и устройствами;  - работа с файлами;  - контроль приложений;  - исключение из событий перехвата | 13 |
| 7 | **Анализ выявленных инцидентов. Подготовка отчетов, классификация угроз и инцидентов**  Специалист должен знать и понимать:  - основные правовые понятия и нормативно-правовые документы, регламентирующие организацию корпоративной защиты от внутренних угроз в хозяйствующих субъектах;  - инструментарий, технологии, их область применения и ограничения при формировании корпоративной защиты от внутренних угроз;  - типовой пакет нормативных документов, необходимого для развёртывания и эксплуатации системы корпоративной защиты в организации;  - виды типовых отчетных форм о выявленных угрозах и инцидентах;  - типы угроз информационной безопасности, понимать их актуальность и степень угрозы для конкретной организации;  - понимать подходы к проведению расследования инцидента информационной безопасности, методики оценки уровня угроз;  - системы DLP и требования по информационной безопасности.  - категорирование информации в РФ.  - юридические вопросы использования DLP-систем: личная и семейная тайны; тайна связи; Специальные технические средства  - меры по обеспечению юридической значимости DLP (Pre-DLP).  - практику право применения при расследовании инцидентов, связанных с нарушениями режима внутренней информационной безопасности (PostDLP).  Специалист должен уметь:  - разрабатывать нормативно-правовые документы хозяйствующего субъекта по организации корпоративной защиты от внутренних угроз информационной безопасности;  - проводить расследования инцидентов внутренней информационной безопасности с составлением необходимой сопроводительной документации;  - создавать отчёты о выявленных инцидентах, угрозах и т.п.  - представлять отчёты руководству, обосновывать полученные результаты анализа. | 2,2 |
| **Всего** | | **40.5** |

**2.2 Защита выпускной квалификационной работы**

2.2.1 Сроки защиты выпускной квалификационной работы

Объем времени и сроки, отводимые на выполнение выпускной квалификационной работы: 2 недели, май, июнь.

Сроки защиты выпускной квалификационной работы: 1 неделя, июнь.

2.2.2 Темы выпускной квалификационной работы

Темы ВКР должны иметь практико-ориентированный характер и должны соответствовать содержанию одного или нескольких профессиональных модулей:

ПМ 01 Техническая эксплуатация инфокоммуникационных сетей связи;

ПМ 02 Техническая эксплуатация инфокоммуникационных систем;

ПМ 03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи;

ПМ 04 Организация производственной деятельности персонала структурных подразделений, отвечающих за предоставление телематических услуг;

ПМ 05 Адаптация конвергентных инфокоммуникационных технологий и систем к потребностям заказчика.

Темы выпускных квалификационных работ с указанием руководителя закрепляются за студентом приказом директора колледжа.

Примерная тематика выпускных квалификационных работ представлена в приложении 2.

**3 ТРЕБОВАНИЯ К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ**

**3.1 Требования к структуре выпускной квалификационной работы**

Структура ВКР должна включать:

- титульный лист;

- индивидуальный график выполнения ВКР;

- задание на ВКР;

- отзыв руководителя ВКР;

- внешняя рецензия;

- пояснительная записка:

- введение с обоснованием актуальности и практической значимости выбранной темы;

- общая часть;

- специальная часть;

- заключение;

- список литературы;

- приложения;

- графическая часть.

Объем ВКР должен быть не менее 30 страниц машинописного текста.

Требования к содержанию разделов выпускной квалификационной работы описаны в Методических указаниях по выполнению выпускной квалификационной работы.

Требования по оформлению выпускной квалификационной работы описаны в Методических рекомендациях по оформлению выпускных квалификационных работ.

**3.2 Условия подготовки и процедура проведения защиты выпускной квалификационной работы**

3.2.1 Условия подготовки выпускной квалификационной работы:

К Государственной (итоговой) аттестации допускается студент, не имеющий академической задолженности и в полном объеме выполнивший учебный план по осваиваемой образовательной программе среднего профессионального образования.

3.2.2 Защита ВКР

Допуск к защите ВКР оформляется приказом директора колледжа.

Защита ВКР проводится на открытом заседании Государственной аттестационной комиссии

На защиту ВКР отводится 45 минут. Процедура защиты:

- доклад студента 10-15 минут;

- чтение отзыва и рецензии (не более 5 минут);

- вопросы членов ГАК и ответы студента (не более 15 минут);

- по желанию (необходимости) выступление руководителя ВКР и рецензента (если они присутствуют на заседании ГАК) с целью защиты, согласия или несогласия с оценкой конкретной ВКР (не более 15 минут).

Заседание ГАК протоколируется. В протоколе записываются:

- итоговая оценка ВКР;

- присуждение квалификации;

- особое мнение членов комиссии.

**4. ОЦЕНКА РЕЗУЛЬТАТОВ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ**

**4.1 Оценка результатов выполнения заданий демонстрационного экзамена**

Оценку выполнения заданий демонстрационного экзамена осуществляет экспертная группа, возглавляемая главным экспертом. Не допускается участие в оценивании заданий демонстрационного экзамена экспертов, принимавших участие в обучении студентов или представляющих с ними одну образовательную организацию.

Состав экспертной группы утверждается руководителем образовательной организации. Количество экспертов, участвующих в оценке демонстрационного экзамена по компетенции 02 Информационные кабельные сети-5 человек, F7 Корпоративная защита от внутренних угроз информационной безопасности – 12 чел.

В ходе проведения демонстрационного экзамена в составе государственной итоговой аттестации председатель и члены государственной аттестационной комиссии присутствуют на демонстрационном экзамене.

Баллы за выполнение заданий демонстрационного экзамена выставляются в соответствии со схемой начисления баллов, приведенной в комплекте оценочной документации. Пример оценочного листа приведен в приложении 3.

Таблица 1.1 – Обобщенная оценочная ведомость по компетенции 02 Информационные кабельные сети

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль задания, где проверяется критерий** | **Критерий** | **Длительность модуля** | **Разделы WSSS** | **Судейские баллы** | **Объективные баллы** | **Общие баллы** |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** |
| **1** | Модуль 2 "Структурированные кабельные системы" | Структурированные кабельные системы | 3:30:00 | 1, 2, 3, 4, 6, 9 | 2,30 | 32,00 | 34,30 |
| **2** | Модуль 3 "Технологии "Умный дом" | Технологии "Умный дом" | 2:30:00 | 1, 7 | 0,00 | 6,90 | 6,90 |
| **Итог** | - | - | 6:00:00 | - | 2,30 | 38,90 | 41,20 |

Таблица 1.2 – Обобщенная оценочная ведомость по компетенции F7 Корпоративная защита от внутренних угроз информационной безопасности

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль, в котором используется критерий** | **Критерий** | **Время выполнен**  **ия**  **Модуля** | **Проверя емые**  **разделы WSSS** | **Баллы** | | |
| **Судейс кие** | **Объек тивн ые** | **Общие** |
|  | 1. Установка и конфигуриро вание компонентов DLP системы | A. Организация работы и управление | 2 часа | 1, 2 | 0 | 18 | 18 |
| B. Установка, конфигурирование и устранение  неисправностей в системе корпоративной защиты от внутренних угроз |
|  | 2. Технологии агентского мониторинга | C. Технологии агентского мониторинга | 1,5 часа | 6 | 0 | 13 | 13 |
|  | 3. Разработка и применение политик, анализ выявленных инцидентов | D. Разработка политик безопасности, анализ выявленных инцидентов | 3 часа | 4, 7 | 0 | 23 | 23 |
| Итого | | | | |  | 54 | 54 |

Необходимо осуществить перевод полученного количества баллов в оценки «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Максимальное количество баллов, которое возможно получить за выполнение задания демонстрационного экзамена, принимается за 100%. Перевод баллов в оценку может быть осуществлен на основе таблицы 2.

Таблица 2 – Перевод баллов в оценку

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Оценка | "2" | "3" | "4" | "5" |
| Отношение полученного количества баллов к максимально возможному (в процентах) | 0,00% - 11,99% | 12,00% - 34,99% | 35,00% - 69,99% | 70,00% - 100,00% |

Таким образом, получаем следующее распределение баллов.

Таблица 3.1 – Перевод баллов в оценку по КОД №1.4 компетенции 02 Информационные кабельные сети

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Оценка ГИА | «2» | «3» | «4» | «5» |
| Количество баллов | 0,00 – 4,93 | 4,94-14,41 | 14,42-28,83 | 28,84-41,2 |

Таблица 3.2 – Перевод баллов в оценку по КОД № 1.1 F7 Корпоративная защита от внутренних угроз информационной безопасности

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Оценка ГИА | «2» | «3» | «4» | «5» |
| Количество баллов | 0,00 –6,47 | 6,48-17,27 | 17,28-35,09 | 35,10-54,0 |

Результаты победителей и призеров чемпионатов профессионального мастерства по компетенциям 02 Информационные кабельные сети, F7 Корпоративная защита от внутренних угроз информационной безопасности, проводимых союзом либо международной организацией «WorldSkills International», осваивающих образовательную программу среднего профессионального образования, засчитываются в качестве оценки «отлично» по демонстрационному экзамену. Условием учета результатов, полученных в конкурсных процедурах, является признанное образовательной организацией содержательное соответствие компетенции результатам освоения образовательной программы в соответствии с ФГОС СПО, а также отсутствие у студента академической задолженности.

**4.2 Оценка выпускной квалификационной работы**

4.2.1 Критерии оценки выпускной квалификационной работы

- соответствие названия работы ее содержанию, четкая целевая направленность;

- логическая последовательность изложения материала;

- необходимая глубина исследования и убедительность аргументации;

- конкретность представления практических результатов работы;

- соответствие оформления выпускной квалификационной работы требованиям ГОСТ Р 705 -2008 и методическим рекомендациям по оформлению выпускных квалификационных работ.

4.2.2 Критерии оценки защиты выпускной квалификационной работы

- четкость и грамотность доклада;

- четкость, внятность, глубина ответов на вопросы присутствующих на заседании ГАК;

- использование технических средств для сопровождения доклада.

4.2.3 Определение окончательной оценки

При определении окончательной оценки за защиту дипломного проекта (работы) учитываются:

- доклад выпускника по каждому разделу выпускной работы;

- ответы на вопросы;

- оценка рецензента;

- отзыв руководителя.

«Отлично» выставляется за следующую выпускную квалификационную работу:

- работа носит исследовательский характер, содержит грамотно изложенную теоретическую базу, глубокий анализ проблемы, характеризуется логичным, последовательным изложением материала с соответствующими выводами и обоснованными предложениями;

- имеет положительные отзывы руководителя и рецензента;

- при защите работы студент показывает глубокие знания вопросов темы, свободно оперирует данными исследования, вносит обоснованные предложения, во время доклада использует презентацию и наглядные пособия (таблицы, схемы, графики и т. п.) или раздаточный материал, легко отвечает на поставленные вопросы.

«Хорошо» выставляется за следующую выпускную квалификационную работу:

- работа носит исследовательский характер, содержит грамотно изложенную теоретическую базу, достаточно подробный анализ проблемы, характеризуется последовательным изложением материала с соответствующими выводами, однако с не вполне обоснованными предложениями;

- имеет положительный отзыв руководителя и рецензента;

- при защите студент показывает знания вопросов темы, оперирует данными исследования, вносит предложения, во время доклада использует презентацию и наглядные пособия (таблицы, схемы, графики и т. п.) или раздаточный материал, без особых затруднений отвечает на поставленные вопросы.

«Удовлетворительно» выставляется за следующую выпускную квалификационную работу:

- носит исследовательский характер, содержит теоретическую главу, базируется на практическом материале, но отличается поверхностным анализом проблемы, в ней просматривается непоследовательность изложения материала, представлены необоснованные предложения;

- в отзывах руководителя и рецензента имеются замечания по содержанию работы и методике анализа;

- при защите студент проявляет неуверенность, показывает слабое знание вопросов темы, не дает полного, аргументированного ответа на заданные вопросы.

«Неудовлетворительно» выставляется за следующую выпускную квалификационную работу:

- не носит исследовательского характера, не содержит анализа проблемы, не отвечает требованиям, изложенным в методических указаниях;

- не имеет выводов либо они носят декларативный характер;

- в отзывах руководителя и рецензента имеются существенные критические замечания;

- при защите студент затрудняется отвечать на поставленные вопросы по теме, не знает теории вопроса, при ответе допускает существенные ошибки, к защите не подготовлены презентация, наглядные пособия или раздаточный материал.

Общая оценка защиты выставляется на закрытом заседании ГАК простым большинством голосов членов ГАК. При равенстве голосов, решение принимает председатель ГАК.

**4.3 Общая оценка государственной итоговой аттестации**

Общая оценка ГИА выставляется по результатам сдачи демонстрационного экзамена и защиты выпускной квалификационной работы.

Общая оценка ГИА выставляется на закрытом заседании ГАК простым большинством голосов членов ГАК. При равенстве голосов, решение принимает председатель ГАК.

По результатам ГИА составляется отчет по итогам работы государственной аттестационной комиссии за подписью председателя ГАК.

**5 ПОРЯДОК АПЕЛЛЯЦИИ И ПЕРЕСДАЧИ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ**

По результатам государственной итоговой аттестации, проводимой с применением механизма демонстрационного экзамена или защиты выпускной квалификационной работы, выпускник имеет право подать в апелляционную комиссию письменное апелляционное заявление о нарушении, по его мнению, установленного порядка проведения государственной итоговой аттестации и (или) несогласии с ее результатами.

Апелляция подается лично выпускником в апелляционную комиссию колледжа.

Апелляция о нарушении порядка проведения итоговой аттестации в форме демонстрационного экзамена подается непосредственно в день проведения. Апелляция о нарушении порядка проведения итоговой аттестации в форме защиты выпускной квалификационной работы подается непосредственно в день проведения защиты.

Апелляция о несогласии с результатами итоговой аттестации подается не позднее следующего рабочего дня после объявления результатов итоговой аттестации.

Апелляция рассматривается не позднее двух рабочих дней с момента ее поступления на заседании апелляционной комиссии. Выпускник, подавший апелляцию, имеет право присутствовать при рассмотрении апелляции. На заседание апелляционной комиссии приглашается председатель соответствующей государственной аттестационной комиссии.

Состав апелляционной комиссии утверждается образовательной организацией одновременно с утверждением состава государственной аттестационной комиссии. Апелляционная комиссия формируется в количестве не менее трех человек из числа преподавателей, имеющих высшую или первую квалификационную категорию, не входящих в данном учебном году в состав государственных аттестационных комиссий. Председателем апелляционной комиссии является директор колледжа.

Рассмотрение апелляции не является пересдачей итоговой аттестации.

При рассмотрении апелляции о нарушении порядка проведения итоговой аттестации апелляционная комиссия устанавливает достоверность изложенных в ней сведений и выносит одно из решений:

- об отклонении апелляции, если изложенные в ней сведения о нарушениях порядка проведения государственной итоговой аттестации выпускника не подтвердились и/или не повлияли на результат государственной итоговой аттестации;

- об удовлетворении апелляции, если изложенные в ней сведения о допущенных нарушениях порядка проведения государственной итоговой аттестации выпускника подтвердились и повлияли на результат государственной итоговой аттестации.

В последнем случае результат проведения государственной итоговой аттестации подлежит аннулированию, в связи с чем протокол о рассмотрении апелляции не позднее следующего рабочего дня передается в государственную аттестационную комиссию для реализации решения комиссии. Выпускнику предоставляется возможность пройти государственную итоговую аттестацию в дополнительные сроки, установленные колледжем.

Для рассмотрения апелляции о несогласии с результатами государственной итоговой аттестации, полученными при защите выпускной квалификационной работы, секретарь государственной аттестационной комиссии не позднее следующего рабочего дня с момента поступления апелляции направляет в апелляционную комиссию выпускную квалификационную работу, протокол заседания государственной аттестационной комиссии и заключение председателя государственной аттестационной комиссии о соблюдении процедурных вопросов при защите подавшего апелляцию выпускника.

Для рассмотрения апелляции о несогласии с результатами государственной итоговой аттестации, полученными при сдаче демонстрационного экзамена, секретарь государственной аттестационной комиссии не позднее следующего рабочего дня с момента поступления апелляции направляет в апелляционную комиссию протокол заседания государственной экзаменационной комиссии, протоколы результатов демонстрационного экзамена выпускника.

В результате рассмотрения апелляции о несогласии с результатами государственной итоговой аттестации апелляционная комиссия принимает решение об отклонении апелляции и сохранении результата государственной итоговой аттестации, либо об удовлетворении апелляции и выставлении иного результата государственной итоговой аттестации. Решение апелляционной комиссии не позднее следующего рабочего дня передается в государственную аттестационную комиссию. Решение апелляционной комиссии является основанием для аннулирования ранее выставленных результатов государственной итоговой аттестации выпускника и выставления новых.

Решение апелляционной комиссии принимается простым большинством голосов. При равном числе голосов голос председательствующего на заседании апелляционной комиссии является решающим.

Решение апелляционной комиссии доводится до сведения подавшего апелляцию выпускника (под роспись) в течение трех рабочих дней со дня заседания апелляционной комиссии.

Решение апелляционной комиссии является окончательным и пересмотру не подлежит.

Студенты, выполнившие выпускную квалификационную работу, но получившие при защите оценку «неудовлетворительно», имеют право на повторную защиту и пересдачу демонстрационного экзамена (не ранее, чем через 6 месяцев после прохождения ГИА впервые).

**Приложение 1а**

**План работы Центра проведения демонстрационного экзамена**

**по КОД № 1.4 по компетенции 02 Информационные кабельные сети**

|  |  |  |
| --- | --- | --- |
| Подготовительный день (С-1) | Время | Мероприятие |
| 08:00 | Получение главным экспертом задания демонстрационного экзамена |
| 08:20 – 08:50 | Проверка готовности проведения  демонстрационного экзамена, заполнение Акта о готовности/не готовности |
| 08:50 – 09:20 | Распределение обязанностей по проведению экзамена между членами Экспертной группы, заполнение Протокола о  распределении ролей |
| 09:20 – 09:50 | Инструктаж Экспертной группы по охране труда и технике безопасности, сбор подписей в Протоколе об ознакомлении |
| 09:50 – 10:20 | Регистрация участников демонстрационного экзамена |
| 10:20 – 10:50 | Инструктаж участников по охране труда и технике безопасности, сбор подписей в Протоколе об ознакомлении |
| 10:50 – 12:00 | Распределение рабочих мест (жеребьевка) и ознакомление участников с рабочими местами, оборудованием, графиком работы, иной документацией и заполнение Протокола |
| День ДЭ (С1) | 08:00 – 09:00 | Печать задания. Ознакомление с заданием и правилами |
| 09:00 – 09:30 | Брифинг экспертов |
| 09:30 – 13:00 | Выполнение задания ДЭ по модулю 2 «Структурированные кабельные сети» |
| 13:00 – 14:00 | Обед |
| 14:00 – 16:30 | Выполнение задания ДЭ по модулю 3  "Технологии "Умный дом" |
| 16:30 – 18:00 | Работа экспертов, заполнение форм и оценочных ведомостей |
| 18:00 – 20:00 | Подведение итогов, внесение главным экспертом баллов в CIS, блокировка, сверка баллов, заполнение итогового протокола |

**Приложение 1б**

**Примерный план работы центра проведения демонстрационного экзамена**

**по КОД №1.1 по компетенции №F7 «Корпоративная защита от внутренних угроз информационной безопасности»**

**(Из КОД)**

|  |  |  |
| --- | --- | --- |
| **День** | **Примерное время** | **Мероприятие** |
| Подготовительный день | 08:00 | Получение главным экспертом задания демонстрационного экзамена |
| 08:00 – 09:00 | Проверка готовности проведения демонстрационного экзамена, заполнение Акта о готовности площадки |
| 09:00 – 09:15 | Распределение обязанностей по проведению экзамена между членами Экспертной группы, заполнение протоколов |
| 09:15– 09:30 | Инструктаж Экспертной группы по охране труда и технике безопасности, сбор подписей в протоколах |
| 09:30– 09:45 | Регистрация участников демонстрационного экзамена |
| 09:45 – 10:15 | Инструктаж участников по охране труда и технике безопасности, сбор подписей в Протоколе об ознакомлении |
| 10:15– 12:00 | Распределение рабочих мест и ознакомление с рабочими местами, оборудованием, графиком работы, иной документацией и заполнение протоколов |
| 12:00 – 16:00 | Подготовка и/или проверка работоспособности площадки в соответствии с заданием |
| День 1 | 08:45 – 09:00 | Ознакомление с заданием и правилами |
| 09:00 – 09:15 | Брифинг |
| 09:15 – 11:15 | Выполнение модуля 1 |
| 11:15 – 11:30 | Перерыв, обработка помещения, проветривание |
| 11:30 – 13:00 | Выполнение модуля 2 |
| 13:00 – 13:45 | Обед, обработка помещения, проветривание |
| 13:45 – 15:30 | Выполнение модуля 3 |
| 15:30 – 15:45 | Перерыв, обработка помещения, проветривание |
| 15:45– 17:00 | Выполнение модуля 3 |
| 17:00 – 19:00 | Работа экспертов, заполнение форм и оценочных ведомостей |
| 19:00 – 20:00 | Подведение итогов, внесение главным экспертом баллов в CIS, блокировка, сверка баллов, заполнение итогового протокола Подготовка площадки для следующей экзаменационной группы (при наличии) |

Если планируется проведение демонстрационного экзамена для двух и более экзаменационных групп (ЭГ) из одной учебной группы одновременно на одной площадке, то это также должно быть отражено в плане.

**Приложение 2**

**Примерная тематика выпускных квалификационных работ**

1. Проектирование абонентского выноса;
2. Проектирование мультисервисного узла доступа (MSAN);
3. Модернизация цифровой АТС с предоставлением услуг пакетной коммутации;
4. Модернизация участка цифровой сети связи;
5. Проектирование цифровой системы передачи (SDH, PDH, DSL);
6. Проектирование транспортной пакетной сети на основе технологии Ethernet;
7. Проектирование сети NGN;
8. Проектирование сети аналогового/цифрового телевидения;
9. Проектирование сети пакетного телевидения IP-TV;
10. Проектирование беспроводной сети передачи данных (WiFi, WiMAX);
11. Проектирование сети абонентского доступа по технологии DSL;
12. Проектирование оптической сети доступа на основе технологии PON;
13. Проектирование ведомственной сети связи предприятия (организации);
14. Моделирование оптической линии связи при помощи САПР;
15. Разработка методического обеспечения для комплексной лаборатории УГКР;
16. Проектирование цифровых радиорелейных линий связи;
17. Проектирование сети абонентского доступа по технологии DECT;
18. Проектирование системы видеонаблюдения;
19. Внедрение новых технологий на сетях связи;
20. Проектирование участка сотовой сети связи;
21. Проектирование виртуальной частной сети;
22. Проект локальной вычислительной сети на симметричных (волоконно-оптических) кабелях;
23. Разработка системы предоставления услуг широкополосного доступа с использованием стандарта WiMAX (или LTE, или еще чего-то) для коттеджного поселка (или еще чего-то);
24. Адаптация методов управления сетью при миграции сетей в сторону пост-NGN, программно-конфигурируемые сети (SDN);
25. Организация транспортной телекоммуникационной сети передачи данных;
26. Разработка электронного учебного пособия по курсу…..
27. Проектирование и монтаж СКС на базе оборудования Nikomax в … аудитории УКРТБ.

**Приложение 3**

**Примерное задание для демонстрационного экзамена**

**по комплекту оценочной документации №1.4 по компетенции 02 Информационные кабельные сети**

**Модуль 2: Структурированные кабельные системы**

**Описание модуля 2 «Структурированные кабельные системы»:**

ФИО участника:

№ рабочего места:

1. Описание задания
   1. Время на выполнение модуля задания: 3 часа 30 минут;
   2. Перед началом монтажа участник должен убедиться, что ему выданы оборудование и материалы в соответствии с перечнем в соответствующем приложении;
   3. В случае выявления дефектов предоставленного оборудования необходимо зафиксировать это в дефектной ведомости;
   4. Уложить кабельные трассы и пучки кабелей в трассах и выполнить их маркировку, а также маркировку пассивных компонентов сети;
   5. Произвести фиксацию пучков;
   6. Произвести монтаж патч-панелей категории 6А, категории 5Е и категории 3;
   7. В выданном бланке необходимо дополнить схемы фасадов телекоммуникационных конструктивов актуальными данными об установленных патч-панелях;

В процессе участникам необходимо соблюдать требования по организации работ, а именно:

* Использовать средства индивидуальной защиты согласно инструкции по ТБ и ОТ;
* Поддерживать чистоту своей рабочей зоны, рабочего места и работать в пределах своей рабочей зоны;
* Бережно относиться к предоставленному оборудованию и материалам.

1. Обобщённая схема оценки
   1. При входе на рабочее место участника эксперты оценивают чистоту рабочего места;
   2. Эксперты оценивают заполнение участником необходимых форм;
   3. Эксперты оценивают качество укладки кабельных трасс, пучков кабелей и отдельных кабелей, а также их маркировку;
   4. Эксперты тестируют изготовленные участником линки, в случае результата PASS для всех портов (допускается 1 ошибка) – Эксперты приступают к оценке качества монтажа соответствующих патч-панелей;
   5. С учётом п. 2.4 Эксперты оценивают качество монтажа патч-панелей: место установки патч-панелей и органайзеров, подвод кабелей к патч-панелям, фиксацию кабелей в органайзерах патч-панелей, маркировку патч-панелей, пучков и кабелей в патч-панелях, качество терминирования модулей, схему терминирования модулей и их установку в патч-панели;
   6. Эксперты оценивают процесс выполнения задания: бережное обращение с предоставленным оборудованием, работа с монтажными инструментами в соответствии с их назначением;
   7. Эксперты оценивают соблюдение участниками инструкции по ТБ и ОТ: использование средств индивидуальной защиты.

### Модуль 3 «Технологии «Умный дом»».

### Описание модуля 3 «Технологии «Умный дом»:

ФИО участника:

№ рабочего места:

1 Описание задания

Время на выполнение модуля задания: 2 часа 30 минут.

Перед началом монтажа участник должен убедиться, что ему выданы оборудование и материалы в соответствии с перечнем в соответствующем приложении;

В случае выявления дефектов предоставленного оборудования необходимо зафиксировать это в дефектной ведомости;

Задание по модулю состоит из следующих последовательно выполняемых шагов.

Шаг 1: Сабнеттинг;

Шаг 2: Монтаж и подключение комплекта видеодомофона;

Шаг 3: Монтаж и подключение IP видеокамеры;

Шаг 4: Монтаж и подключение устройств домашней автоматизации на объекте «Квартира».

**Примерное задание для демонстрационного экзамена**

**по комплекту оценочной документации №1.1 по компетенции №F7«Корпоративная защита от внутренних угроз информационной безопасности»**

Модули с описанием работ

Модуль 1: Установка и конфигурирование компонентов DLP системы

Введение

В компания «Демо Лаб» возникла необходимость внедрения DLP системы для лучшей защиты разработок и предотвращения утечек прочей информации.

Вам необходимо установить и настроить компоненты системы в соответствии с выданным заданием.

Основными каналами потенциальной утечки данных являются носители информации, электронная почта и различные интернет-ресурсы.

Серверные компоненты устанавливаются в виртуальной среде, сетевые интерфейсы настроены, но IP адреса нужно назначить согласно прилагаемой карточке. Подготовлены следующие виртуальные машины для дальнейшей работы:

AD Сервер с контроллером домена

DLP сервер установлен (но не настроен), активирована лицензия

Виртуальная машина для установки сервера агентского мониторинга

Виртуальные машины «нарушителей» для установки агентов

В компании развернут домен со всеми сотрудниками с указанием ФИО, должности и контактов. До установки системы необходимо подготовить доменных пользователей в соответствии с заданием.

Для большей сетевой безопасности в компании все устройства должны иметь статический IP-адрес. Сетевые настройки указаны в дополнительных сведениях к заданию.

Стоит отметить, что имена всех компьютеров (hostname) должны быть уникальными в соответствии с номером рабочего места (например, server-16).

При выполнении заданий можно пользоваться справочными ресурсами в сети Интернет и документацией на компьютерах в общем сетевом каталоге.

Все дистрибутивы находятся в каталоге, указанном в дополнительной карточке задания.

Все логины, пароли, сетевые настройки и прочее указаны в дополнительной карточке задания

Если в задании указано сделать скриншот, необходимо называть его по номеру задания, например: Задание\_5\_копирование.jpg.

Задание 1: Настройка контроллера домена

Необходимо создать и настроить следующих доменных пользователей с соответствующими правами:

Логин: user1, пароль: 12345678, запретить локальный вход в систему

Логин: user2, пароль: 12345678, запретить локальный вход в систему

Логин: user3, пароль: 12345678, права администратора домена и локального администратора

Логин: user4, пароль 12345678, права пользователя домена

Задание 2: Настройка DLP сервера

DLP-сервер контроля сетевого трафика уже предустановлен, но не настроен.

Необходимо вычислить IP-адрес сервера через локальную консоль виртуальной машины.

Настроить DNS на сервере для корректной работы.

Необходимо проверить наличие активной лицензии и в случае ее отсутствия обратиться к экспертам.

Необходимо синхронизировать каталог пользователей и компьютеров LDAP с домена с помощью ранее созданного пользователя.

Для входа в веб-консоль необходимо использовать ранее созданного пользователя домена с полными правами на администрирование системы, полный доступ на все области видимости.

Запишите IP-адреса, токен, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные вами) вашей системы в текстовом файле «отчет.txt» с заголовком IWTM.

Корректно выполненным заданием будет являться работоспособная система с верно настроенными параметрами.

Задание 3: Установка и настройка сервера агентского мониторинга

Необходимо ввести сервер в домен от ранее созданного пользователя, после перезагрузки войти в систему от этого пользователя (продолжить работу в домене).

Установить базу данных с паролем суперпользователя 12345678.

Установить сервер агентского мониторинга с параметрами по умолчанию.

При установке необходимо установить соединение с DLP-сервером контроля сетевого трафика по IP-адресу и токену, но можно сделать это и после установки сервера агентского мониторинга.

Настроить пользователя консоли управления: officer с паролем 12345678.

Синхронизировать каталог пользователей и компьютеров с Active Directory.

После синхронизации настроить вход в консоль управления от ранее созданного пользователя, установить полный доступ к системе, установить все области видимости.

Зафиксировать факт создания пользователя и настройку скриншотом.

Проверить работоспособность входа в консоль управления без ввода пароля. Стоит обратить внимание, что если сервер не введен в домен, данная опция работать не будет.

Зафиксировать факт подключения без пароля скриншотом.

Запишите IP-адреса, логины и пароли от учетных записей, а также все прочие нестандартные данные (измененные вами) вашей системы в текстовом файле «отчет.txt» с заголовком IWDM.

Задание 4: Установка агента мониторинга на машине нарушителя

Необходимо ввести клиентскую машину в домен от ранее созданного пользователя, после перезагрузки войти в систему от этого пользователя (продолжить работу в домене).

Установить агент мониторинга с помощью задачи первичного распространения с сервера агентского мониторинга. Необходимо учесть, что установка осуществляется только с правами администратора (доменного или локального). Ручная установка с помощью создания пакета установки является неверным выполнением задания.

Зафиксировать успешное выполнение задачи скриншотом

В случае проблем стоит проверить настройки брандмауэра и DNS.

Задание 5: Установка и настройка подсистемы сканирования сетевых ресурсов (Crawler)

Необходимо установить и настроить подсистему сканирования сетевых ресурсов на сервер с установленным сервером агентского мониторинга.

Необходимо создать общий каталог Share в корне диска и установить права доступа на запись и чтение для всех пользователей.

Необходимо настроить подсистему сканирования сетевых ресурсов на автоматическое ежедневное сканирование только ранее созданного каталога.

Зафиксировать выполнение задания скриншотом настройки в webконсоли.

Стоит учесть, что неправильная настройка DNS на серверных машинах, а также неправильные настройки брандмауэра могут привести к неработоспособной системе сканирования сетевых ресурсов.

Задание 6: Проверка работоспособности системы

Необходимо создать проверочную политику на правило передачи, копирования, хранения и буфера обмена (все 4 варианта срабатывания событий) для данных, содержащих слово «Экзамен», установить низкий уровень угрозы для всех событий, добавить тег «Экзамен».

Проверить срабатывание всеми четырьмя возможными способами (передачи, копирования, хранения и буфера обмена, хотя бы 1 событие на каждый тип) с помощью виртуальной машины нарушителя с установленным агентом.

Сделать одну выборку, в которой будет отображено только по одному событию каждого типа (суммарно 4 события: передачи, копирования, хранения и буфера обмена).

Зафиксировать выполнение скриншотом выполненной выборки или конструктора выборки.

Задание 7: Защита системы с помощью сертификатов

Создайте цифровой сертификат (дерево сертификатов) формата PKCS для защиты веб-соединения с DLP-сервером по протоколу HTTS. Сертификат и используемый ключ должен удовлетворять общепринятым на сегодня стандартам и требованиям (по длительности, длине ключа и т.п.), параметры сертификата должны соответствовать атрибутам компании. Утилита для создания сертификата – на выбор участника из доступных в операционных

системах и дистрибутивах (openssl или аналоги).

Дерево сертификатов должно включать:

• корневой root-сертификат (ca)

• сертификат сервиса (веб-сайта)

Итоговый результат должен включать:

• Дерево из 2 (3)-х сертификатов, упакованных в пакет PKCS (.p12), а также представленные в виде отдельных файлов ключей и сертификатов.

• Содержимое команд по генерации ключей и сертификатов в текстовом файле «отчет.txt»

• Скриншоты успешного подключения к консоли сервера DLP без ошибок сертификата, скриншоты окон просмотра сертификата в системе просмотра сертификатов Windows (закладки «Общие», «Путь сертифкации»).

Сертификаты не должны содержать ошибок, предупреждений (warnings), неверной информации о компании Demo.lab и т.п.

Генерацию сертификатов зафиксируйте скриншотами.

Модуль 2: Технологии агентского мониторинга

Задания выполняются только с помощью компонентов DLP системы (не групповыми политиками или аналогичными решениями).

Все сценарии заданий (где применимо) необходимо воспроизвести и зафиксировать результат.

Называйте созданные вами разделы/политики/группы и т.д. в соответствии с заданием, например «Политика 1» или «Правило 1.2» и т.д.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). В этом случае необходимо протоколировать свои результаты с помощью двух скриншотов для каждого задания (скриншот заданной политики и скриншот ее работы). Для некоторых

заданий необходимо после фиксации результатов в виде скриншотов удалить заданную политику, что будет оговорено отдельно в тексте задания.

Все скриншоты необходимо сохранить в папке «Модуль 2».

Формат названия скриншотов политик:

Пример 1 для сохранения скриншота созданной политики: CP-1.jpg

где СP – сокращение от англ. сreating а policy, 1 – номер задания

Пример 2 для сохранения скриншота работающей политики: PW-1.jpg

где PW – сокращение от англ. policy work, 1 – номер задания.

Пример 3 для сохранения нескольких скриншотов одной работающей политики:

PW-1-2.jpg

где PW – сокращение от англ. policy work, 1 – номер задания; 2 – номер

скриншота для задания 1.

Задание 1

Необходимо создать новую политику, применить ее к группе компьютеров по умолчанию. Последующие правила по заданиям должны быть добавлены в эту политику.

Зафиксировать выполнение скриншотом.

Задание 2

Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления сервером агентского мониторинга на машину нарушителя для удаленного доступа к серверу агентского мониторинга.

Проверить работоспособность, зафиксировать выполнение скриншотом запущенной консоли с указанием адреса.

Задание 3

Для удаленного управления необходимо создать дополнительного локального офицера безопасности для доступа к серверу агентского мониторинга с полными правами на управление и просмотр разделов.

Имя пользователя: user1, пароль: 12345678

Проверить работоспособность с удаленной консоли, установленной ранее, зафиксировать выполнение скриншотом.

Задание 4

Необходимо запретить пользоваться Microsoft Paint, так как участились случаи подделки печатей компании.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 5

Необходимо запретить создание снимков экрана в табличных процессорах для предотвращения утечки секретных расчетов и баз данных.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 6

Необходимо поставить на контроль буфер обмена в текстовых процессорах.

Проверить работоспособность и зафиксировать выполнение занесением пары событий в веб-консоль DLP-сервера на любые политики. Также подтвердить выполнение скриншотом.

Задание 7

Необходимо запретить печать на сетевых принтерах. Зафиксировать создание политики скриншотом.

Задание 8

Необходимо запретить запись файлов на все съемные носители информации (флешки), оставив возможность чтения и копирования с них. Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 9

С учетом ранее созданной политики необходимо разрешить запись файлов на доверенный носитель. Запрет на запись на остальные носители оставить в силе.

Проверить работоспособность и зафиксировать настройку и выполнение скриншотами.

Задание 10

Создать политику по блокировке копирования файлов формата zip на USB-накопители.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 11

Необходимо поставить на контроль печать документов на принтерах.

Продемонстрировать работоспособность на любую из политик.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 12

Необходимо установить контроль за компьютером потенциального нарушителя в случае использования браузера путем создания снимков экрана каждые 15 секунд или при переходе на другую страницу.

Проверить работоспособность и зафиксировать выполнение:

продемонстрировать, что снимки экрана из задания появляются в веб-консоли DLP-сервера. Подтвердить выполнение задания скриншотами.

Задание 13

Заблокируйте доступ к CD/DVD на клиентском компьютере (виртуальной машине).

Проверить работоспособность и зафиксировать выполнение скриншотом.

Задание 14

Осуществить выдачу временного доступа (30 минут) клиенту до заблокированного CD привода.

Зафиксировать скриншотами факт выдачи доступа и необходимые действия для выдачи доступа.

Задание 15

На машине нарушителя необходимо запретить использование буфера обмена при подключении к удаленным машинам по протоколу RDP.

Проверить работоспособность и зафиксировать выполнение

скриншотом.

Задание 16

Необходимо установить (сменить) пароль для удаления агента мониторинга на машине нарушителя с помощью средств сервера агентского мониторинга (удаленно).

Проверить работоспособность и зафиксировать выполнение Скриншотом

Модуль 3: Разработка и применение политик, анализ выявленных инцидентов

Введение

Создайте в DLP-системе политики безопасности согласно нижеперечисленным заданиям.

Политики должны автоматически блокировать трафик и/или предупреждать о нарушении в соответствии с заданием.

Для некоторых политик необходима работа с разными разделами консоли управления: категориями и терминами, технологиями, объектами защиты и т. п. Способ, которым создана корректная политика, оставлен на усмотрение самого экзаменуемого.

При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием (если в задании это не указано явно, необходимо самостоятельно задать уровень угрозы).

Списки сотрудников, занимаемые позиции и отделы сотрудников представлены в разделе «Персоны» по результатам LDAP-синхронизации с AD-сервером компании. После создания всех политик может быть запущен автоматический «генератор трафика», который передаст поток данных, содержащих как утечки, так и легальную информацию.

При правильной настройке политики должны автоматически выявить (или блокировать) и маркировать инциденты безопасности. Не должно быть ложных срабатываний, т. к. легальные события не должны маркироваться как вредоносные. Не должно быть неправильной маркировки. Должны быть выявлены все инциденты безопасности.

Проверьте синхронизацию времени на всех системах, т. к. расхождение во времени между системами может повлиять на актуальность событий.

Для некоторых политик могут понадобиться дополнительные файлы, которые можно найти в папке «Additional files» в общей папке из дополнительных сведений.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). В этом случае необходимо протоколировать свои результаты с помощью двух скриншотов для каждого задания (скриншот заданной политики и скриншот ее работы). Для некоторых заданий необходимо после фиксации результатов в виде скриншотов удалить заданную политику, что будет оговорено отдельно в тексте задания.

Все скриншоты необходимо сохранить в папке «Модуль 3».

Формат названия скриншотов политик:

Пример 1 для сохранения скриншота созданной политики: 01-CP.jpg

где СP – сокращение от англ. сreating а policy, 01 – номер задания

Пример 2 для сохранения скриншота работающей политики: 04-PW1.jpg, 04-PW-2.jpg, где PW – сокращение от англ. policy work, 04 – номер задания, 1,2 – номер скриншотов

Задания на разработку политик можно выполнять в любом порядке.

ВНИМАНИЕ!

Необходимо называть политики / объекты / категории / теги и прочее

ТОЛЬКО в соответствии с номером и названием задания

Политики — Политика X, например «Политика 4».

Для комбинированных политик формат: Политика 4.1, 4.2 и т.д.

Объект защиты — Объект X, например «Объект 11».

ВНИМАНИЕ!

Все политики «по умолчанию», находящиеся в консоли управления в процессе выполнения заданий должны быть отключены или удалены, так как могут помешать корректной оценке.

ВНИМАНИЕ!

25

При разработке и тестировании политик стоит учитывать, что нарушителем могут являться не только указанные в задании пользователи, а еще и виртуальная машина с агентом мониторинга.

ВНИМАНИЕ!

При разработке политик стоит учитывать, что все политики трафика могут передаваться как через веб-сообщения, так и через почтовые сообщения.

В случае, если данный пункт не соблюден, то проверка заданий может быть невозможной.

Задание 1

Создайте локальную группу пользователей «Сотрудники под наблюдением». Добавьте в нее трех любых пользователей. Подтвердите выполнение задания скриншотами.

Задание 2

Для работы системы необходимо настроить периметр компании:

Почтовый домен: demo.lab.

Список веб ресурсов необходимо создать и назвать «Доверенные домены»: worldskills.org, filialdemo.lab, demolab-info.ru, dlpsystems.lab.

Группа персон 1: пользователи домена.

Исключить из перехвата почту генерального директора.

Подтвердите выполнение задания скриншотами.

Задание 3

Для недавно нанятого аудитора компании необходимо создать пользователя системы с правами доступа только на чтение и выполнение отчетов, сводок и событий, а также на просмотр каталога локальных и доменных пользователей без возможности редактирования. Области

видимости: все.

Логин: auditor, пароль: 12345678

Подтвердите выполнение задания скриншотами.

Политика 4

В связи с секретностью при организации очередного WorldSkills, совет директоров решил контролировать передачу информации о WorldSkills за пределы компании. В связи с этим необходимо создать политику на правило передачи текстовых данных за пределы компании (на адреса вне домена), содержащих слова «ВорлдСкиллз», «WorldSkills».

Hеобходимо учесть, что в словах могут содержаться комбинации латиницы и кириллицы, а также стоять пробел между словами, например:

«Ворлд Skills». Ложных срабатываний быть не должно (например, просто на Ворлд или Skills).

Вердикт: разрешить √

Уровень нарушения: средний •

Тег: мобильники

Проверить работоспособность.

Политика 5

Для контроля за движением официальных документов необходимо вести наблюдение за передачей как пустых, так и заполненных шаблонов документа за пределы компании. Стоит учесть, что содержимое документа может изменяться в пределах 50%.

Для пустого документа:

Вердикт: разрешить √

Уровень нарушения: нет

Тег: договор

Для заполненного документа:

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: договор

Проверить работоспособность.

Политика 6

Для мониторинга движения анкет необходимо вести наблюдение за анкетами компании, запрещая любую внешнюю передачу документов, содержащих заполненные бланках, при этом пустые бланки контролировать не нужно.

Вердикт: запретить ×

Уровень нарушения: средний •

Тег: бланк

Проверить работоспособность.

Политика 7

Для мониторинга движения официальных документов необходимо вести наблюдение за документами компании с официальной печатью. При этом совет директоров и генеральный директор могут отправлять эти документы без ограничений.

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: печать

Проверить работоспособность.

Политика 8

В компании происходит передача сообщений, содержащих специальные коды доступа к внутренней информационной системе. Все коды находятся в документе «Коды компании» (10 штук). Необходимо контролировать коды внутри компании, но запрещать передачу за пределы.

Передача кодов внутри компании:

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: коды

Передача кодов за пределы компании:

Вердикт: запретить ×

Уровень нарушения: средний •

Тег: бланк

Проверить работоспособность.

Политика 9

Ракетное вооружение для авиационных комплексов различного класса, в разработке которого участвует компания, планируется к внедрению в эксплуатацию. Информация о технике может иметь конфиденциальный и секретный характер, хотя и не содержать гриф.

Необходимо блокировать любые попытки передачи данных об этих объектах на внешние адреса. Технические объекты задаются буквенноцифирными кодами на русском языке:

Р-Цифры-Буквы или РЦифрыБуква или Р-ЦифрыБуква

• Р – русская буква «Р»

• Цифры – не более 4-х подряд, например, 27 или 5000 (обязательно

наличие хотя бы одной цифры)

• Буквы – от 1 до 2-х подряд, например, Р-27АЭ

Вердикт: запретить ×

Уровень нарушения: высокий •

Тег: ракеты

Проверить работоспособность.

Политика 10

Сотрудники отдела ИТ заподозрены в сливе баз данных клиентов. Необходимо настроить мониторинг выгрузок из БД для контроля движения данных из базы данных страховых компаний только при отправке из отдела информатизации.

Вердикт: разрешить √

Уровень нарушения: средний •

Тег: база

Проверить работоспособность.

Политика 11

В связи с постоянными заказами на транспортировку больших грузов, сотрудники компании подрабатывают в тайне от начальства, занимаясь попутной перевозкой других грузов, а также пассажиров. В связи с этим необходимо отслеживать в почтовых сообщениях упоминания об автостопе, халтуре, подработке, грузовом такси.

Вердикт: разрешить √

Уровень нарушения: средний •

Тег: подработка

Проверить работоспособность.

Политика 12

Необходимо запретить передачу документов с грифом (информационной меткой) «ООО Demo Lab. Конфиденциально» или «ООО Demo Lab. Строго конфиденциально» любым сотрудникам за пределы

компании. Обратите внимание, что при вводе информационной метки с клавиатуры сотрудники могут ошибаться и вводить между словами более 1 пробела или табуляции, а также писать название компании на русском языке, например, «OOO Demo Лаб», «ООО Демо Лаб».

Вердикт: запретить ×

Уровень нарушения: высокий •

Тег: печать

Проверить работоспособность.

Политика 13

В связи с распространением коронавирусной инфекцией сотрудники стали чаще обсуждать различные новости, мешая рабочему процессу.

Необходимо отслеживать следующие термины: COVID, COVID-19, коронавирус, коронавирусная инфекция.

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: вирус

Проверить работоспособность.

Политика 14

Для защиты персональных данных сотрудников необходимо запрещать всем, кроме отдела кадров передавать информацию, содержащую данные паспортов (в том числе и сканы/фото), а также СНИЛС и ИНН.

Вердикт: запретить ×

Уровень нарушения: высокий •

Тег: пдн

Проверить работоспособность.

Политика 15

Необходимо контролировать передачу документов формата электронных таблиц (исключая csv файлы!), а также CAD-документации.

Стоит учесть, что файлы могут передаваться в том числе и на съемных носителях информации.

Вердикт: разрешить √

Уровень нарушения: низкий •

Тег: печать

Проверить работоспособность.

Задание 16: Анализ инцидентов, обычные сводки

Создайте новую вкладку сводки в разделе «Сводка» под названием «Экзамен» и создайте в ней 4 виджета:

Динамика активности по событиям за последнюю неделю

Статистика по политикам за последние 7 дней

По типу событий: необработанные нарушения за три дня

По топ-нарушителям за текущий месяц.

Задание 17: Анализ инцидентов, специальные выборки

Необходимо создать новую вкладку в разделе «Сводка» под названием «Особые выборки» и добавить в нее виджеты:

Отображающий события с уровнем угрозы от низкого до высокого на правила копирования (внешние носители, печать) за последние 7 дней.

Отображающий события с любым одним тегом.