КОНКУРСНОЕ ЗАДАНИЕ

ДЛЯ VI ОТКРЫТЫЙ ОТБОРОЧНЫЙ ЧЕМПИОНАТ ГУАП
В ОЧНОМ ФОРМАТЕ
КОМПЕТЕНЦИИ
«КОРПОРАТИВНАЯ ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»
ДЛЯ ОСНОВНОЙ ВОЗРАСТНОЙ КАТЕГОРИИ
17-35 лет

Конкурсное задание включает в себя следующие разделы:

Форма участия:

Индивидуальная

Общее время выполнения задания:

18 часов

Конкурсное задание:

Модуль B: Установка и настройка системы

Описание

В компания «Демо Лаб» возникла необходимость внедрения DLP системы InfoWatch Traffic Monitor **версии 6.11** для лучшей защиты разработок и предотвращения утечек прочей информации.
Ваша задача – установить указанные компоненты IWTM используя распределенный сценарий установки.
Основными каналами потенциальной утечки данных являются носители информации, электронная почта и различные интернет-ресурсы.
Серверные компоненты устанавливаются в виртуальной среде _____,
сетевые интерфейсы полностью настроены (но IP адреса нужно назначить согласно прилагаемой карточке). Подготовлены следующие виртуальные машины для дальнейшей работы:

1. AD Сервер с контроллером домена
2. DLP IWTM установлен (но не настроен), активирована лицензия
3. Виртуальная машина для установки системы IWTM Device Monitor Server
4. 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 карточкой задания**.
Для большей сетевой безопасности в компании нет DHCP сервера, поэтому все устройства должны иметь статический IP-адрес. Адреса всех устройств необходимо выбрать самостоятельно и записать их в отчет. Сетевые настройки указаны в дополнительных сведениях к заданию.
Стоит отметить, что имена компьютеров (hostname) должны быть уникальными.

Модуль B: Установка, конфигурирование и устранение неисправностей в системе систем корпоративной защиты от внутренних угроз

Задание 1: Настройка InfoWatch Traffic Monitor

Для входа в консоль (веб-интерфейсу) InfoWatch Traffic Monitor используйте нового доменного пользователя (_____).

Необходимо синхронизировать каталог пользователей и компьютеров LDAP с домена. Для синхронизации пользователей и компьютеров необходимо использовать подразделение "_____". Остальные каталоги импортировать не нужно. Рекомендуется для LDAP-синхронизации создать специального доменного пользователя с ограниченными правами (_____), у которого будет отключена возможность локального входа в домен (см. карточку доп. сведений).

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

Задание 2: Настройка Домена demo.lab

Необходимо создать доменных пользователей и настроить их в соответствии с карточкой дополнительных сведений.

Обратите внимание на ограничение прав пользователей

Задание 3: Установка и настройка InfoWatch Device Monitor

Установите и настройте IWDM

Необходимо ввести Windows Server DM (**IWDM-Server**) в домен

Установить базу данных PostgreSQL

Установить InfoWatch Device Monitor с параметрами по умолчанию, в качестве базы данных использовать ранее установленную базу данных PostgreSQL.

При установке необходимо настроить пользователя для доступа к консоли управления: officer с паролем _____

После установки использовать доменного пользователя для входа в консоль управления (_____)

Синхронизируйте IWDM с Active Directory (компьютеры и пользователи) и свяжите IWDM с вашим InfoWatch Traffic Monitor.

Настройки сетевых интерфейсов указаны в дополнительных сведениях.

Задание 4: Установка InfoWatch Device Monitor Agent

Необходимо создать доменных пользователей для клиентских машин (см. карточку). Ввести виртуальную машину нарушителя в домен и войти в систему от ранее созданного доменного пользователя.

Установите InfoWatch Device Monitor Agent на виртуальные машины-нарушителя

- На 1-ю пользовательскую машину – с помощью задачи первичного распространения (без формирования пакета установки) в Device Monitor Server.
- На 2-ю пользовательскую машину – с помощью групповых политик домена. Политика должна применяться только на конкретную машину.

Важно! Плюсом будет реализация всех действий при включенном Брандмауэре Windows, не снижая защищенность системы. Для корректной работы необходимо настроить Брандмауэр (и другие необходимые для этого подсистемы) для взаимодействия компонент IWDM/IWTM.
Проверьте работоспособность IWDM агента.

Задание 5: Установка и настройка подсистемы Crawler
Необходимо установить и настроить подсистему Crawler на Windows Server IWMD. Создайте общий доступ только на каталог c:\data\share на Windows Server IWDM с правами чтения и записи для всех.
Настройте Crawler на автоматическое ежедневное сканирование только ранее созданного каталога вашего Windows Server и зафиксируйте выполнение задания скриншотом настройки crawler в web-консоли IWTM.
Плюсом будет реализация всех действий при включенном Брандмауэре Windows. Для корректной работы необходимо настроить Брандмауэр/групповые политики для взаимодействия компонент IWDM/IWTM.
Задание 6: Проверка работоспособности системы
Необходимо создать проверочную политику в InfoWatch Traffic Monitor на правило передачи, копирования, хранения и буфера обмена (все 4 варианта срабатывания событий) для данных, содержащих слово «_____», установить низкий уровень угрозы для всех событий, добавить тег «_____».
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.

Задание 7: Безопасность домена Windows
1. Для минимизации возможностей пользователей по изменению настроек систем, отключить панель управления компьютером для пользователей ИТ-отдела.
2. Для повышения безопасности настройте для всех сотрудников (кроме директора и глав отделов), пароли пользователя длинной не менее 8 и их смену раз в три месяца.
3. Локализовать с помощью групповых политик использование установочных файлов (.exe) на компьютерах домена в папке allowexe (на диске C:). В

остальных папках блокировать запуск исполняемых файлов. Политика не должна навредить запуску системным приложениям Windows, Program Files и т.п.

Задание 8: Развертывание DLP уровня сети. InfoWatch Traffic Monitor.

Динамичное развитие компании Demo.Lab привело к значительному расширению штата (+600 человек) и переезду в новый офис.
В связи с этим, принято решение о переносе всей ИТ-инфраструктуры компании, в том числе и систем обеспечения корпоративной безопасности в облако. Это, с одной стороны, решает вопросы с организацией дистанционного доступа к инфраструктуре для сотрудников, с другой – консолидирует всю ИТ-инфраструктуру, повышая надежность и доступность.
Необходимо мигрировать решение InfoWatch Traffic Monitor (IWTM), согласно рекомендациям, полученным от подразделений внедрения ГК Инфовотч. Основная идея – максимальное разнесение компонент уровня сети (network, IWTM) и хоста (endpoint, IWDM) для распределения нагрузки в связи с увеличением числа сотрудников.
По возможности все настройки и события в системе (как IWTM, так и IWDM) необходимо сохранить при миграции.
Системными администраторами компании в облаке уже развернуты:

- контроллер домена (с каталогом Active Directory),
- почтовый сервер (частично настроен)
- прокси-сервер (требует сетевой настройки)

В соответствии с Вашей частью пилотного проекта на отдельном сегменте сети «песочницы» Заказчика необходимо разнести на 3 разных машины следующие сетевые компоненты InfoWatch Traffic Monitor:

- Основной сервер безопасности IWTM (Node)
- База данных IWTM (Database)
- Вспомогательный сервер IWTM (Sniffer) для приема копии трафика с виртуального коммутатора

Ваша задача – установить указанные компоненты IWTM используя распределенный сценарий установки (см рис. 1).

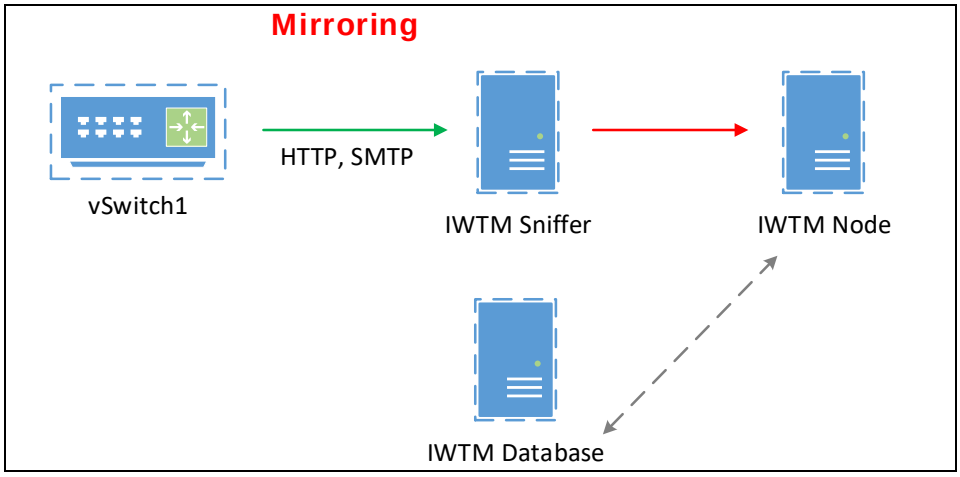

Рисунок 1. Схема развертывания DLP уровня сети.

Необходимо мигрировать Node или Database сервер на отдельную машину с сохранением базы данных на отдельной машине, установить и настроить перехватчик сетевого трафика (Sniffer) на отдельный сервер, у которого есть 2 сетевых интерфейсы (для управления и перехвата трафика).
Все развернутые сервера должны быть доступны для управления (службы) и мониторинга из консоли управления IWTM.

Задание 9: Подготовка Active Directory

Если не создано ранее, для дальнейших работ необходимо создать и настроить несколько специализированных пользователей в Active Directory:

- _____ (права локального администратора)
- _____ (права пользователя домена, отключить возможность локального входа в домене)
- _____1, 2 (машина нарушителя, права пользователя домена)

Ваша задача – создать вышеперечисленных пользователей в соответствии с указанными условиями.

Задание 10: Развертывание DLP уровня хоста. InfoWatch Device Monitor.

В соответствии с Вашей частью пилотного проекта сети Заказчика необходимо (а) либо развернуть с нуля (б) либо произвести миграцию следующих endpoint-компонент InfoWatch Device Monitor (IWDM):

- Основной сервер безопасности IWDM (Node)

- База данных IWDM (Database). Сохранение всех событий и конфигураций будем значительным плюсом.
- Агент IWDM на машину «нарушителя» (WIN-CLI)

Ваша задача – установить указанные компоненты IWDM на виртуальные машины (см рис. 2).

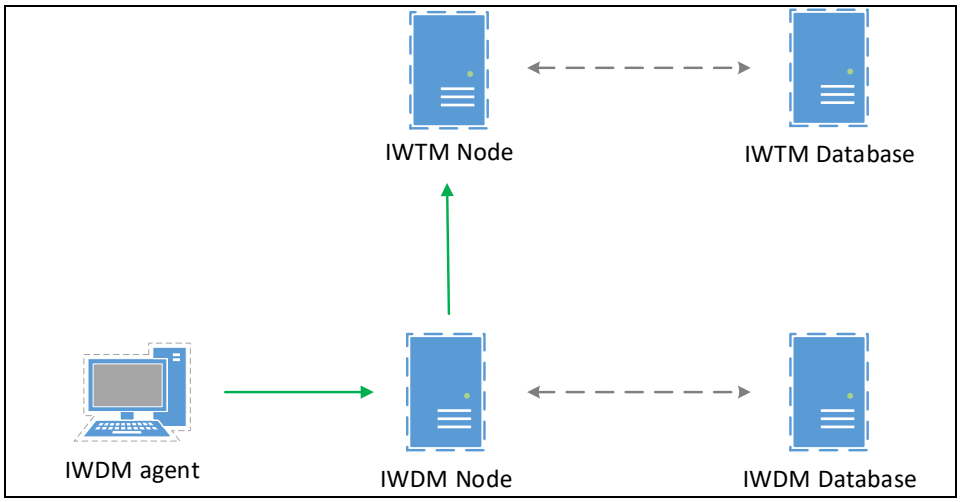

Рисунок 2. Схема развертывания DLP уровня хоста (+ интеграция с DLP уровня сети).

Осуществите интеграцию сервера безопасности IWDM с Active Directory.

Задание 11: Подключение источников информации для DLP уровня сети. Корпоративный почтовый сервер (в разрыв).

Необходимо показать Заказчику возможность перехвата почты с внутреннего почтового сервера компании. Для этого в «песочнице» заранее развернут корпоративный почтовый сервер iRedMail (уже интегрирован с Active Directory). Ваша задача – интегрировать IWTM с iRedMail (см. рис 5).

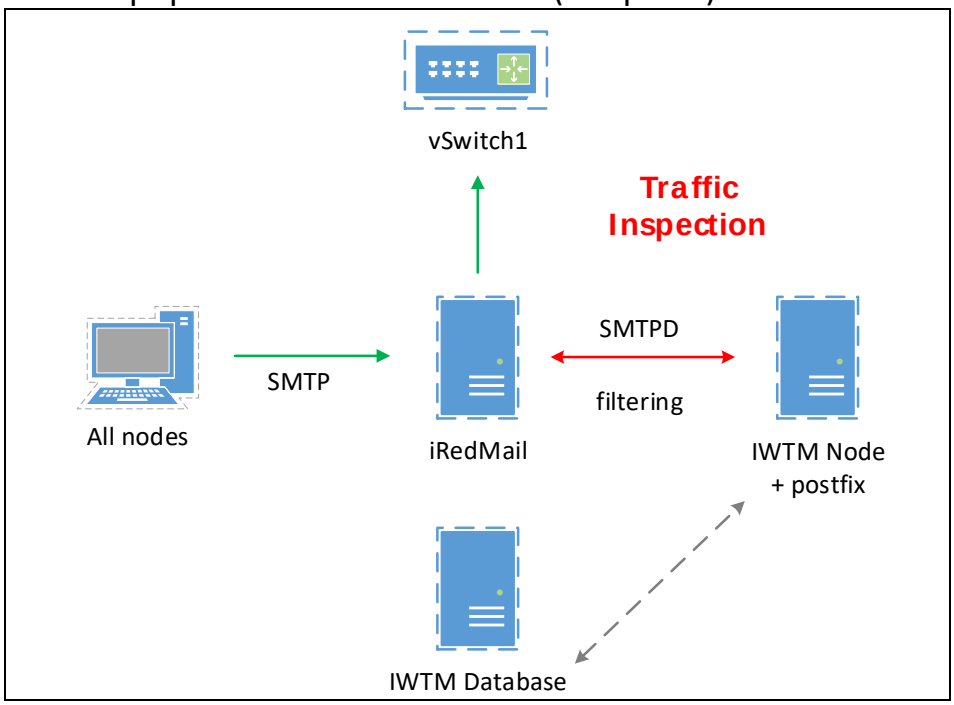

Рисунок 5. Схема интеграции SMTP в разрыв.

Задание 12: Беспарольное SSH-соединение защищенного доступа к IWTM

Для удаленного управления IWTM Node настройте безопасный беспарольный (по сертификату) доступ по SSH (используя программу PuTTY, с помощью RSA-ключа) с контроллера домена (Domain Controller).

Также необходимо настроить межсерверный доступ по SSH с IWTM Node на IWTM Sniffer с помощью ключей.

Модуль D. Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз

ВНИМАНИЕ! Необходимо называть политики/объекты/категории/тэги и т.п. **ТОЛЬКО** в соответствии с номером и названием задания

Политики — Политика XX, например «**Политика 4**». Для комбинированных политик формат: **Политика 4.1**, **Политика 4.2** и т.д.
Объект защиты — Объект и XX, например «**Объект 11**».

Ошибки в названиях приводят к снижению баллов или даже к невозможности проверки. При выполнении задания учитывайте, что совместно с созданными могут срабатывать стандартные политики, что необходимо предотвратить.

ВНИМАНИЕ! **ВСЕ политики «по-умолчанию»,** находящиеся в IWTM на момент старта соревнований**, должны быть отключены или удалены**

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

Задание 1

Создайте локальную группу пользователей «_____» в Traffic Monitor. Добавьте в нее пользователя _____.

Задание 2

Для работы системы необходимо настроить периметр компании:

- Домен: demo.lab.
- Список веб ресурсов: _____. Необходимо создать новый список ресурсов, назвав его «_____».
- Группа персон 1: _____.
- Группа персон 2: группа «_____.»
- Исключить из перехвата _____.

Задание 3

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

Политика 4

В связи с постоянными проблемами при организации очередного чемпионата WorldSkills (Корпоративный Чемпионат ООО Demo.lab), совет директоров решил

контролировать передачу информации о WorldSkills и Корпоративном Чемпионате за пределы компании до окончания соревнований. В связи с этим необходимо создать политику в InfoWatch Traffic Monitor на правило передачи текстовых данных за пределы компании (на адрес вне домена), содержащих слова «ВорлдСкиллз», «WorldSkills», «_____». Сделать исключение на доменную зону _____.

Необходимо учесть, что в словах могут содержаться комбинации латиницы и кириллицы, а также стоять или не стоять пробел между словами, например: «Ворлд скиллз». Ложных срабатываний быть не должно (например, просто на World или Skills).

Разрешить передачу, установить средний уровень угрозы. Тег «Политика 4».

Политика 5

Для контроля за движением официальных документов необходимо вести наблюдение за передачей как пустых, так и заполненных шаблонов документа (шаблон — «Договор компании.doc») за пределы компании. Стоит учесть, что содержимое документа может изменяться в пределах ____%.

Уровень угрозы низкий, не блокировать, тег и название «Политика 5.1».

*В случае, если в документе присутствует фамилия генерального директора, выставить уровень угрозы средний, **не блокировать**, тег и название «Политика 5.2».*

Политика 6

Для мониторинга движения анкет необходимо вести наблюдение за анкетами с печатью компании за пределы компании, запрещая любую внешнюю передачу документов, содержащих печать компании в пустых и заполненных бланках «анкета участника.docx».

При этом бланки без печати или просто печать не контролировать.

Генеральный директор и совет директоров могут обмениваться данной информацией совершенно свободно.

*Печать + бланк: Уровень угрозы средний, **блокировать**, тег «Политика 6».*

Политика 7

В связи с санкциями и растущим курсом валют, компания ООО Demo Lab решила сэкономить и закупила программное обеспечение на компьютеры сотрудников у китайских партнеров. Проконсультировавшись с отделом безопасности, руководство компании выяснило, что отдел закупок пошел на большие риски – китайское ПО собирает огромное количество аналитических сведений о машинах, на которых оно работает. Дабы предотвратить какие-либо утечки, необходимо заблокировать доступ к поддоменам, собирающим аналитику:

«_____»; запретить отправку данных за пределы компании, содержащую информацию о «железе» - упоминания AMD, Intel, Байкал, _____, _____ в любом регистре.

*Уровень угрозы средний, **блокировать**, тэг «Китайцы». Проверку проводить при отправке на почтовые домены.*

Политика 8

У генерального директора компании недавно появился котик и его фото утекло в сеть компании. Теперь сотрудники обмениваются смешными картинками с подписями и масками внутри компании и выкладывают их в социальные сети. Директор решил, что его котик вызвал снижение качества работы сотрудников из-за повышенной милоты картинок и хочет запретить обмен фотографией котика. Необходимо запретить обмен фотографией и немного измененной фотографией котика (до ≈____%) как внутри компании, так и за ее пределы, установить низкий уровень угрозы, тег «Политика 8». Фотография котика есть в дополнительных данных.

Политика 9

Дочерняя компания «ООО Повозка» занимается транспортировкой грузов в разные города. Каждому рейсу присваивается уникальный идентификационный номер по следующему шаблону «3 буквы (латиница, любой регистр) - (знак дефиса) номер груза (от 0 до 1000, исключая несчастливые номера: 666 и 13) . (точка) 2 буквы (кириллица, верхний регистр)
Например: jDt-123.УЛ , kdU-665.ЪЩ
Не должно быть срабатывания на несчастливые номера грузов (например: kdO-666.Д или jfd-13.ЮШ).
Уровень угрозы средний, не блокировать, тег «Политика 9».

Политика 10

Из-за пандемии коронавирусной инфекции к сезону отпусков было решено отслеживать информацию, которая может содержать в себе слова, так или иначе относящиеся к отпуску, так как некоторые сотрудники могут вернуться на рабочее место из отпуска потенциально зараженными. Список слов (во всех формах), которые стоит учитывать: море, отпуск, курорт, _____, и названия популярных российских курортов и городов для отпуска летом (Крым, Сочи, Анапа, _____ и прочее

Уровень угрозы средний, не блокировать, тег «COVID», тэг «Развлечение»

Политика 11

По причине пандемии коронавирусной инфекции решено выявлять потенциально опасных с инфекционной точки зрения сотрудников (заболевших, находились в

контакте и т.п.), некоторые из которых могут скрывать эти факты, чтобы не проиграть по зарплате. Отслеживать сообщения, которые могут содержать в себе слова, так или иначе относящиеся к заболеванию: COVID (внутри любой фразы), SARS (внутри любой фразы, например SARS-CoV-2), _____ (внутри любой фразы, учитывать морфологию).
Уровень угрозы средний, не блокировать, тег «Политика 10», «COVID».

Политика 12

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. Критичными данными в выгрузке являются телефоны, ИНН, и _____и в 1 документе присутствует **___ или более** компаний. Для настройки используйте файл «Выгрузка из БД.csv».
Уровень угрозы средний, блокировать, тег «Политика 12».

Политика 13

Было замечено, что сотрудники компании стали получать множество рекламных сообщений электронной почты, из-за чего возникла необходимость отследить потенциальную утечку баз email адресов сотрудников. В связи с этим необходимо детектировать сообщения, содержащие адреса электронной почты доменов компании
Уровень угрозы средний, не блокировать, тег «Политика 13».

Политика 14

При переезде в новый просторный офис, компанией ООО Demo Lab был расширен штаб сотрудников – было решено взять несколько десятков выпускников технических вузов на стажировку. Для того, чтобы они работали более эффективно, директор компании предложил отслеживать доступ сотрудникам, работающим в отделе ИТ, доступ к основным социальным сетям и анонимным имиджбордам – vk.com, ok.ru, t.me, _____, _____, _____.

Контроль для тестовых целей установить за **электронными письмами** в эти доменные зоны.

Уровень угрозы средний, детектировать, тег «Развлечение».

Модуль Е. Технологии защиты и анализа сетевого трафика

Задание 1: Настройка сетевого окружения и компонентов систем

С помощью технологии виртуальных машин _____ для выполнения задания смоделирована корпоративная сеть организации на 2 филиалах.

При выполнении заданий необходимо ключевые настройки (установка паролей, настройки соединения с БД, компрометация, скриншоты работоспособной сети ViPNet и аналогичные) или указанные моменты в задании подтверждать скриншотами.

В ходе выполнения данного задания нужно установить основное ПО VipNet на рабочие станции будущей защищенной сети.

Доступ на все Windows 10: без пароля

Доступ на все Windows Server: xxXX1234

Все пароли пользователей в сети ViPNet сделать 12341234

Все пароли администраторов в сети ViPNet сделать xxXX1234.

Перед установкой ПО ViPNet необходимо настроить сеть в соответствии со схемой. Если машины для координаторов не маршрутизирует пакеты между интерфейсами, необходимо включить эту опцию самостоятельно.

Задание 1.1. Установка по VIPNET administrator для создания защищённой сети:

- Установить и настроить рабочее место администратора VipNet (на базе виртуальной машины Net1-Admin (ЦО)): Центр управления сетью (серверное и клиентское приложение ЦУС), Удостоверяющий и ключевой центр (УКЦ).

Задание 1.2. Установка ПО ViPNet Coordinator и ПО VipNet Client на соответствующие виртуальные машины:

- На компьютере на Net1-Admin (ЦО) установить ПО ViPNet Client (Windows), рабочее место администратора;
- На компьютере на Net1-Coord (ЦО) установить ПО ViPNet Coordinator (Windows);
- На компьютере на Net2-Coord (Филиал) установить ПО ViPNet Coordinator (Windows);
- На ВМ на Net2-Client (филиал) установить ПО ViPNet Client, рабочее место пользователя;

Задание 2. Защита локально-вычислительной сети предприятия с применением ПО ViPNet

Необходимо использовать рабочее место администратора (созданное ранее) для создания структуры защищенной сети, развернуть с помощью технологии виртуальных машин _____ сеть предприятия и настроить необходимые АРМ в соответствии с заданными ролями.

Схема сети, которую требуется создать, приведена далее.

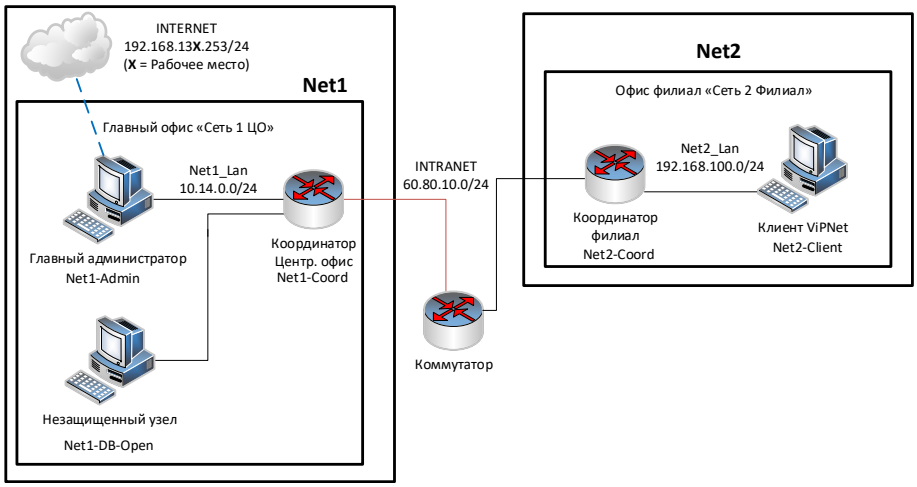

Рисунок 1 Схема защищенной сети

В итоге выполнения задания должны быть развернуты и настроены следующие сетевые узлы защищенной сети (см. таблицу).

Таблица 1 Узлы защищенной сети если УКЦ и ЦУС на одной машине.

Вирт. машина	Название сетевого узла	ПО VipNet	ОС сетевого узла	Имя пользователя сетевого узла, уровень полномочий
Net1-Admin (ЦО)	Главный администратор (VM)	ViPNet Administrator (ЦУС клиент и сервер + УКЦ) ViPNet Client	ОС Windows Server	Admin
Net1-Coord (ЦО)	Координатор Центр Офис (VM)	ViPNet Coordinator	ОС Windows 10	CoordinatorOffice
Net2-Coord (Филиал)	Координатор Филиал (VM)	ViPNet Coordinator	ОС Windows 10	CoordinatorSub
Net2-Client (филиал)	Пользователь_2 Филиал	ViPNet Client	ОС Windows 10	User2

Вирт. машина	Название сетевого узла	ПО VipNet	ОС сетевого узла	Имя пользователя сетевого узла, уровень полномочий
	(VM)			

Связи между узлами необходимо настроить самостоятельно.

Таблица 2. Схема связей пользователей

Схема связей пользователей	Coordinator Office	Admin	Coordinator Subsidiary	User2
CoordinatorOffice				
Admin				
CoordinatorSub				
User2				

Задание 2.1. Создание структуры защищенной сети:

- ЦУС. Необходимо создать в ЦУС структуру защищенной сети в соответствии с заданной схемой (**выгрузить отчет в HTML**). Создать пользователей узлов, настроить полномочия пользователей и их связи в соответствии со схемой.
- УКЦ. Провести инициализацию УКЦ, сохранить контейнер ключей администратора в общей папку (создать подпапку Задание 2.1), поменять тип паролей для пользователей («собственный»). Задать пароли пользователей и сохранить в текстовый файл. Сформировать дистрибутивы ключей для всех сетевых узлов (сохранить на жесткий диск). Создать группы узлов для центрального офиса и филиала, настроить пароль администратора группы сетевых узлов для каждой из групп (проверить, что пароль работает).
- На всех узлах сети корректно настроить или проверить корректность настройки сетевых интерфейсов в соответствии со схемой (на координаторах 2 интерфейса – внешний и внутренний), проверить доступность соседних узлов.
- Разнести DST файлы по АРМ, провести первичную инициализацию узлов защищенной сети (координаторов и клиентов), проверить доступность узлов защищенной сети и сделать скриншоты работоспособности узлов.

Задание 2.2. Компрометация узла защищенной сети

Перед началом выполнения зафиксировать скриншотами имеющуюся структуру сети и окно УКЦ с вариантами персонального ключа компрометируемого пользователя, т. к. в случае неудачной компрометации структура сети может нарушиться.

Произвести компрометацию ключей и восстановление сетевого взаимодействия средствами УКЦ/ЦУС:

- скомпрометировать ключи пользователя user 2 на узле Пользователь_2 Филиал
- произвести смену ключей пользователя и сетевых узлов,
- отправить обновления и произвести процедуру смены ключа пользователя на узле Пользователь_2 Филиал (фиксировать все шаги),
- проверить работу защищенной сети после обновления отправив сообщение от пользователя user 2 администратору.

Восстановление взаимодействия с помощью ручной установки DST засчитано не будет.

Задание 2.3. Модификация защищенной сети

Перед началом выполнения сделать Snapshot всех модифицируемых машин.

Модификация структуры сети:

- Добавить новый сетевой узел _____ и пользователя _____ за координатором ЦентрОфис (без фактического развертывания его на виртуальной машине). Добавить связь пользователя нового узла с пользователем user2. На указанных узлах проверить появление нового узла.
- Добавить пользователя _____ на узле Пользователь_2 Филиал (Net2-Client филиала 2), связать его со всеми пользователями группы узлов центральный офис. Для указанных пользователей проверить появление новой связи.
- Отправить письмо по Деловой почте пользователю _____ с узла admin.

Задание 3. Межсетевое взаимодействие защищённых сетей (со связями «все со всеми»)

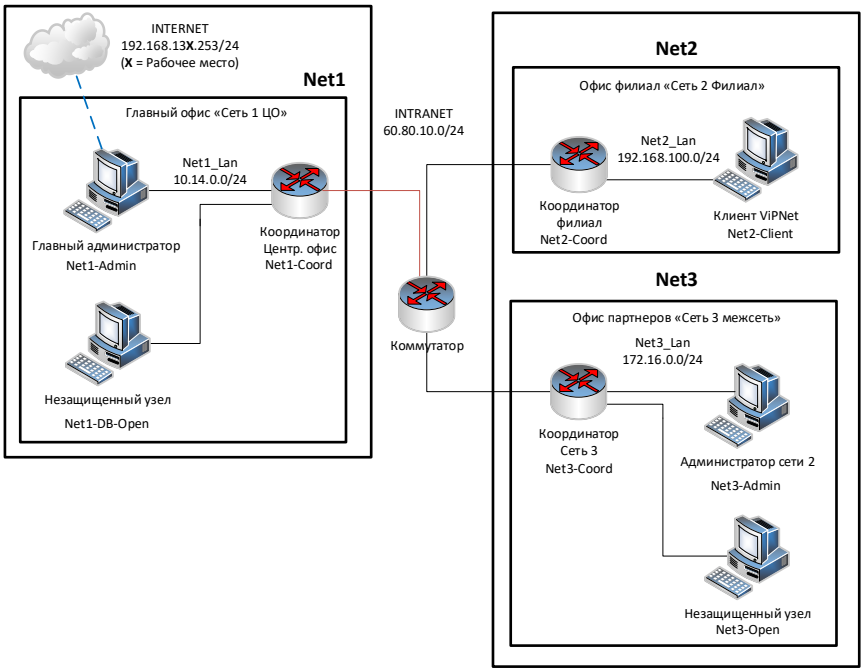

Рисунок 2 Схема межсетевого взаимодействия

Развернуть на Net3-Admin (Сеть 3 межсеть) на ПК рабочее место Администратора партнёрской сети, создать структуру второй сети:

- Рабочее место администратора (БД, ЦУС, УКЦ, ViPNet Client)
- 1 координатор (Net3-Coord)
- 1 узел Admin и пользователь Admin

Все пароли пользователей в сети ViPNet сделать 12344321

Пароли администраторов сети ViPNet сделать xxXX1234

- Установить и настроить необходимое ПО
- Настроить межсетевое взаимодействие между двумя защищёнными сетями, сделать скриншоты всех этапов установки межсетевого взаимодействия.
- Проверить взаимодействие узлов, отправив сообщение деловой почты в программе ViPNet Client Monitor с узла Admin (сеть 1) на Admin (сеть 2).

Задание 4. Туннелирование в рамках межсетевого взаимодействия

- Подключить незащищенную машину в сети 3 (Net3-Client-Open).
- Для второй открытой машины использовать Net1-DB-Open узел в сети 1
- Настроить туннелирование таким образом, чтобы взаимодействие между открытыми узлами из разных сетей осуществлялось по шифрованному

каналу. Проверить доступность незащищённых машин друг другу с помощью ICMP (ping).

Модуль F: Технологии защиты узла и агентского мониторинга

Задание 1

Необходимо установить (сменить) пароль для удаления Device Monitor Agent всех виртуальных машин нарушителей с помощью средств DeviceMonitor Server (удаленно). Пароль: _____

Задание 2

Необходимо создать новую политику (кроме политики на устройства по умолчанию), назвав ее «_____», применить ее к группе компьютеров по умолчанию.

Последующие правила по заданиям должны быть добавлены в эту политику.

Задание 3

Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления IWDM на компьютер «нарушителя» для удаленного доступа к серверу IWDM.

Задание 4

Используйте для входа в консоль IWDM доменного пользователя _____.

Задание 5

Необходимо запретить пользоваться Microsoft Paint, а также Paint 3D (при наличии), так как участились случаи подделки печатей компании.

Задание 6

Необходимо запретить создание снимков экрана в табличных процессорах (Libre Office calc) и калькуляторе для предотвращения утечки секретных расчетов и баз данных.

Задание 7

Необходимо поставить на контроль буфер обмена в офисных приложениях пакета Libre Office (writer и impress), а также notepad++.

Проверить работоспособность и зафиксировать выполнение занесением пары событий в IWTM на любые политики Traffic Monitor.

Задание 8

Необходимо поставить на контроль копирования данных до ___ Мб на USB-накопители и сетевые папки.

Проверить работоспособность любым способом и зафиксировать выполнение занесением пары событий в IWTM на любые политики Traffic Monitor.

Задание 9

Создать политику по блокировке копирования исполняемых exe-файлов на USB-накопители. Проверить работоспособность и зафиксировать выполнение (зафиксировать результаты в виде скриншотов), _____

Задание 10

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

Задание 11

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

Задание 12

Для предотвращения неэффективного расхода рабочего времени сотрудников отслеживать движение видео контента (*.avi, *.mov, *.mp4) в общих папках компании. Отдельно контролировать файлы больше ___Мбайт и меньше ___ Мбайт.

Задание 13

Необходимо установить контроль за компьютером потенциального нарушителя в случае использования браузера Google Chrome путем создания снимков экрана каждые 15 секунд или при смене окна.

Задание 14

Задание …

Модуль G: Предотвращение инцидентов и управление событиями информационной безопасности

Задание 1: сводки

Создайте новые вкладки сводки в разделе «Сводка» под названием «Чемпионат» и «_____»

Задание 2: сводки

Создайте в сводке «Чемпионат» 2 виджета:

- Выборка по событиям краулера за _____
- Выборка по политикам с технологиями: графические объекты, _____, _____за последние _____

Задание 3: Отчеты

Создайте отчет в разделе «Отчеты», назвав его «_____» и добавьте 2 виджета:

- Отобразить всех пользователей, занимающихся не относящейся к работе деятельностью (по тегам или другим критериям из задания на политики)
- Вычислить топ-5 нарушителей среди всех сотрудников компании

Задание 4

Необходимо создать виджет в разделе «Сводка», вкладка «_____», отображающий события с уровнем угрозы от низкого до высокого на правила копирования (внешние носители, печать) за последние __ дня(/дней).

Задание 5

Необходимо создать виджет в разделе «Сводка», вкладка «_____» для отображения нарушений только от обоих компьютеров нарушителей (виртуальные машины) со средним и _____ уровнем угрозы за последние __ дня(/дней).

Модуль 2. Исследование (аудит) организации с целью защиты от внутренних угроз.

- Задания должны быть выполнены в виде отчёта в формате .odt или.docx; Графические иллюстрации должны быть внутри документа.
- Итоговый скан документа (с подписью участника) должен быть загружен на платформу file.worldskills.ru под названием ***Модуль_2_Аудит_<Фамилия участника>.расширение***

Участника самостоятельно распечатывает документ, проверяет, расписывается, сканирует и загружает pdf-отчёт на платформу file.worldskills.ru. Работа не принимается к оценке без наличия скан копии с подписью конкурсанта.

Задание. Подготовка аудита информационной безопасности организации

В целях выполнения подготовительных работ для построения Модели угроз информационной безопасности планируется провести аудит информационных систем и процессов организации.

Вам, как специалисту, поручено провести подготовительные мероприятия по подготовке аудита информационной безопасности информационной системы по исходным данным и основываясь на действующих требованиях Российского законодательства по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну. В процессе проведения аудита **вы должны решить следующие задачи (задания)**:

1.1 Определить перечень основных объектов информатизации, представленных в организации.

1.2 Определить каналы передачи данных

1.1 Определить перечень субъектов, имеющих доступ к информации, на основании данных Таблицы 1, структура компании и личным опытом работы с AD

1.2 Определить границы доменов доверия (периметр(ы) безопасности).

1.3 Осуществить категорирование (классификацию) представленной в организации информации в соответствие с типами информации ограниченного доступа

Информация	Тип информации ограниченного доступа	Субъекты, имеющие доступ к информации	Комментарии

1.4 Определить перечень актуальных для организации объектов защиты, привести обоснование. Заполнить таблицу.

Объект информатизации	Объект защиты	Обоснование актуальности защиты	Тип объекта защиты согласно определения в ГОСТ Р 50922-2006

1.5 Провести сопоставление типов информации ограниченного доступа ограниченного доступа требованиям законодательства РФ. Идентифицировать перечень нормативно-правовых актов (НПА) РФ и регуляторных документов, требования которых распространяются на организацию. Заполнить таблицу.

Информация	Тип информации ограниченного доступа	НПА и регуляторные документы

1.6 Составьте перечень основных угроз (рисков) от внутренних утечек информации ограниченного доступа для организации. Приведете пояснения, при необходимости. Рассмотреть только случай, когда

источник угрозы безопасности информации (субъект) – внутренний нарушитель, физическое лицо.

…..
……
…..

Приложение 1. Результаты опроса сотрудников и руководства

Направления работ

Научно-исследовательская компания «Демо Лаб» заказала демоверсию DLP-системы с целью опробовать функциональные возможности программного обеспечения.
Компания «Демо Лаб» занимается (а) контрактной разработкой и (6) продажей перспективных электронных систем в интересах государственных и коммерческих организаций. Также в партнёрстве с компаниями «большой четверка» компания (в) осуществляет аудит сторонних организаций (в части стандартов качества и т. п.), обладая всеми необходимыми для этого лицензиями.

Доходность работ по направлениям

Маржинальность работ, связанных с контрактной разработкой различного рода систем (НИР/НИОКР) составляет 20%, от продаж электронной компонентной базы (собственной и сторонней разработки) – 50%, от аудиторской деятельности – 50%.
Средняя стоимость контракта на разработку – 100 млн рублей (всего за 1 контракт), средний период исполнения - 2 года. В год заключается, в среднем, 20 контрактов.
Тематики работ носят несекретный, но закрытый характер, например: разработка перспективных систем космической связи, радиолокационных станций, систем связи, систем автоматизации для органов государственной власти и т. п.
Средняя стоимость договора поставки электронных компонент – 20 000 долларов, длительность поставки – 2 недели. В год 2000 «средних продаж».
Договора по участию в аудиторской деятельности приносят 1 млн. $ в год.
Также у компании есть договор с государственными органами об организации государственных закупок по отдельным категориям продуктов путём организации торгов (т. е. компания действует как оператор торгов). В рамках организации торгов компания занимается сбором заявок, предоставляемых участниками торгов в соответствии с правилами организованных торгов в соответствии с требованиями 325-ФЗ. Данная деятельность убыточна для организации, но положительно сказывается на её репутации.

ИСХОДНЫЕ ДАННЫЕ

Примечание: Сформулированные исходные данные организации в точности соответствуют базе данных организации, расположенной на сервере AD.

Структура компании

Группа ТМ	**Кол-во сотрудников**	**Информационные системы**	**Циркулирующие данные**
Бухгалтерия (Accounting)	8		
Отдел договоров (Financial)	10		
Совет директоров (BOD)	3		
Отдел кадров (HR)	3		
Информационные технологии (IT)	10		
Отдел продаж (Sales)	15		
Тендерный комитет (Tenders)	7		

Таблица 1

В AD компании для каждого сотрудника указаны следующие атрибуты:

1. Фотография
2. Фамилия
3. Имя
4. Должность
5. Отдел
6. Электронная почта

7. Мобильный телефон
8. Skype/WhatsApp