|  |  |
| --- | --- |
|  |  |

КОНКУРСНОЕ ЗАДАНИЕ КОМПЕТЕНЦИИ

«КОРПОРАТИВНАЯ ЗАЩИТА

ОТ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

*Регионального* Чемпионата по профессиональному мастерству «Профессионалы» в 2024 г.

2024 г.

Конкурсное задание разработано экспертным сообществом и утверждено Менеджером компетенции, в котором установлены нижеследующие правила и необходимые требования владения профессиональными навыками для участия в соревнованиях по профессиональному мастерству.

**Конкурсное задание включает в себя следующие разделы:**

[1. ОСНОВНЫЕ ТРЕБОВАНИЯ КОМПЕТЕНЦИИ 3](#_Toc142037183)

[1.1. Общие сведения о требованиях компетенции 3](#_Toc142037184)

[1.2. Перечень профессиональных задач специалиста по компетенции «\_\_\_\_\_\_\_\_\_» 3](#_Toc142037185)

[1.3. Требования к схеме оценки 5](#_Toc142037186)

[1.4. Спецификация оценки компетенции 5](#_Toc142037187)

[1.5. Конкурсное задание 6](#_Toc142037188)

[1.5.1. Разработка/выбор конкурсного задания 6](#_Toc142037189)

[1.5.2. Структура модулей конкурсного задания (инвариант/вариатив) 7](#_Toc142037190)

[2. СПЕЦИАЛЬНЫЕ ПРАВИЛА КОМПЕТЕНЦИИ 8](#_Toc142037191)

[2.1. Личный инструмент конкурсанта 8](#_Toc142037192)

[2.2.Материалы, оборудование и инструменты, запрещенные на площадке 8](#_Toc142037193)

[3. ПРИЛОЖЕНИЯ 8](#_Toc142037194)

**ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ**

*Пример:*

1. *ИТ – информационные технологии*
2. *ИБ – информационная безопасность*
3. *НСД – несанкционированный доступ*
4. *ИС – информационная система*
5. *IPS – система предотвращения вторжений*
6. *ТК – требования компетенции*
7. *КЗ – конкурсное задание*
8. *ИЛ – инфраструктурный лист*
9. *КО – критерии оценки*
10. *ПЗ – план застройки площадки компетенции*
11. *VPN – виртуальные частные сети (англ. Virtual Private Networks)*
12. *DLP – система защиты от утечек данных   
    (англ. Data Leakage Prevention)*
13. *СОВ – система обнаружения вторжений*
14. *IDS – система обнаружения вторжений   
    (англ. Intrusion Detection System)*
15. *IPS – система предотвращения вторжений   
    (англ. Intrusion Prevention System)*
16. *NGFW – межсетевой экран следующего поколения   
    (англ. Next Generation Firewall)*

1. ОСНОВНЫЕ ТРЕБОВАНИЯ КОМПЕТЕНЦИИ

1.1. ОБЩИЕ СВЕДЕНИЯ О ТРЕБОВАНИЯХ КОМПЕТЕНЦИИ

Требования компетенции (ТК) «КОРПОРАТИВНАЯ ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» определяют знания, умения, навыки и трудовые функции, которые лежат в основе наиболее актуальных требований работодателей отрасли.

Целью соревнований по компетенции является демонстрация лучших практик и высокого уровня выполнения работы по соответствующей рабочей специальности или профессии.

Требования компетенции являются руководством для подготовки конкурентоспособных, высококвалифицированных специалистов / рабочих и участия их в конкурсах профессионального мастерства.

В соревнованиях по компетенции проверка знаний, умений, навыков и трудовых функций осуществляется посредством оценки выполнения практической работы.

Требования компетенции разделены на четкие разделы с номерами и заголовками, каждому разделу назначен процент относительной важности, сумма которых составляет 100.

1.2. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ ЗАДАЧ СПЕЦИАЛИСТА ПО КОМПЕТЕНЦИИ «КОРПОРАТИВНАЯ ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

*Перечень видов профессиональной деятельности, умений и знаний, и профессиональных трудовых функций специалиста (из ФГОС/ПС/ЕТКС.) и базируется на требованиях современного рынка труда к данному специалисту*

*Таблица №1*

**Перечень профессиональных задач специалиста**

|  |  |  |
| --- | --- | --- |
| **№ п/п** | **Раздел** | **Важность**  **(%)** |
| **1** | **Организация работы и охрана труда** | **4%** |
| 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; |  |
| **2** | **Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от угроз информационной безопасности** | **21%** |
| 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; * Модели контроля и управления доступом; * 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, VMWare Workstation; * 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 Windows Server Linux (в т.ч. в защищенных отечественных ОС, таких как Astra Linux); * 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; * Устанавливать и настаивать системы корпоративной защиты по отечественными операционными системами, такими как AstraLinux. * Настройка защищенного домена Windows, групповые политики AD; * Создание и установка цифровых сертификатов; * Настройка защищенного соединения между элементами сетевой инфраструктуры: SSH, HTTPS и т.п. |  |
| **3** | **Обследование объекта информатизации** | **7%** |
| Специалист должен знать и понимать:   * Типовые организационно-штатные структуры организаций различных сфер деятельности и размера; * Типовой набор объектов защиты, приоритеты доступа к информации, типовые роли пользователей; * Каналы передачи данных: определение и виды; * Подходы и методы обследования объекта информатизации для последующей защиты; * Сетевые устройства, которые могут быть использованы как источники событий для анализа; * Формирование процессов и процедур аудита ИБ. * Обследование корпоративных информационных систем. * Состояние корпоративной информации. * Инструменты и технологии обеспечения корпоративной защиты от внутренних угроз. * Критерии эффективности проекта по обеспечению корпоративной защиты от внутренних угроз. * Препятствия реализации проектов по обеспечению корпоративной защиты от внутренних угроз. |  |
| Специалист должен уметь:   * Проводить обследование корпоративных информационных систем. * Самостоятельно изучить структуру организации на основании полученных материалов; * Определить объекты защиты, роли пользователей, права доступа; * Выявить потоки передачи данных и возможные каналы утечки информации; * Создать объекты защиты и политику ИБ, используя технологии анализа в системе корпоративной защиты; * На основании собственного анализа, уметь связать требования нормативной базы, структуру организации, выявленные угрозы, объекты, роли безопасности для построения актуальных политик безопасности; * Задокументировать и уметь представить результаты обследования (аудита), включая потоки данных, потенциальные каналы утечек, роли пользователей, объекты защиты и т.п. |  |
| **4** | **Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз** | **17%** |
| 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, Google Talk, 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; |  |
| **5** | **Технологии анализа и защиты сетевого трафика** | **28%** |
| Специалист должен знать и понимать:   * Организационно-технические и правовые основы использования электронного документооборота в информационных системах; * Структуру виртуальной защищенной сети. Назначение виртуальной защищенной сети. Особенности построения VPN-сетей. Основные типы классификаций VPN-сетей * Технологии построения виртуальных защищенных сетей на основе программных и программно-аппаратных решений; * Ключевые компоненты VPN-сетей; * Особенности VPN-сети и механизмы их управления; * Современные криптографические алгоритмы. Криптопровайдеры, криптографические интерфейсы и библиотеки; * Архитектура, основные компоненты PKI их функции и взаимодействие; * Жизненный цикл ключей и сертификатов; * Электронный сертификат ключей ЭЦП. Формирование, подписание и использование сертификатов; * Защита видео и конференций приложений; * Назначение и основные сценарии применения IDS-технологий; * Архитектуру и особенности внедрения IDS-технологий; * Распространённые вектора атак и уязвимости современных корпоративных информационных систем. |  |
| Специалист должен уметь:   * Осуществлять развёртывание и администрирование VPN-сетью (добавление, удаление, изменение объектов сети, настройка параметров работы, контроль работоспособности и др.). Обновление ПО, установленного на узлах защищенной с0435ти. * Работать и удостоверяющей и ключевой информацией. Формирование и управление ключевой структурой сети. Издание и управление сертификатами пользователей. * Настраивать защиту сегментов IP-сетей, координация работы узлов защищенной сети. Защиты трафика, передаваемого по открытым каналам связи; * Осуществлять защиту оконечных рабочих мест; Контроль пользовательских приложений; * Реализовывать межсетевое взаимодействие и туннелирование; * Компрометация рабочих мест; * Обеспечение межсетевого экранирования и криптографической защиты информации; * ПО для электронного документооборота в VPN-системах * Защита систем, обеспечивающих поддержку процессов   информационного взаимодействия   * Устанавливать и конфигурировать современные IDS-системы корпоративного класса в сети предприятия; * Выполнять настройку и проверку работоспособности; * Проводить детектирование атак (потенциальных угороз) в ручном, автоматизированном и автоматическом режиме; * Проводить правильную классификацию уровня угрозы инцидента; * Использовать базы контентной фильтрации; * Использовать дополнительные модули анализа информационных потоков, если это продиктовано особенностями условий ведения бизнеса; |  |
| **6** | **Технологии агентского мониторинга** | **14%** |
| Специалист должен знать и понимать:   * Функции агентского мониторинга; * Общие настройки системы агентского мониторинга; * Соединение с LDAP-сервером и синхронизация с Active Directory; * Политики агентского мониторинга, особенности их настройки; * Особенности настроек событий агентского мониторинга; * Агентские политики DLP; * Механизмы диагностики агента, подходы к защите агента. * Групповые политики различных ОС; * Мандатные и ролевые модели доступа; * Возможности встроенных средств защиты ОС. |  |
| 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. * Защитать системы от эксплуатации уязвимостей средствами ОС * Разработка и реализация групповых политик; * Возможности встроенных средств защиты ОС. |  |
| **7** | **Анализ событий информационной безопасности и подготовка отчетов** | **9%** |
| 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 (Post-DLP). |  |
| 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. |  |
| **Всего** | | **100%** |

1.3. ТРЕБОВАНИЯ К СХЕМЕ ОЦЕНКИ

Сумма баллов, присуждаемых по каждому аспекту, должна попадать в диапазон баллов, определенных для каждого раздела компетенции, обозначенных в требованиях и указанных в таблице №2.

*Таблица №2*

**Матрица пересчета требований компетенции в критерии оценки**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Критерий/Модуль** | | | | | | | | **Итого баллов за раздел ТРЕБОВАНИЙ КОМПЕТЕНЦИИ** |
| **Разделы ТРЕБОВАНИЙ КОМПЕТЕНЦИИ** |  | **A** | **Б** | **В** | **Г** | **Д** | **Е** |  |
| **1** | 0,5 | 1 | 0,5 | 0,5 | 0,5 | 0,5 | 3,5 |
| **2** | 15,5 |  | 2,5 | 1 | 2,5 |  | 21,5 |
| **3** |  | 7 |  |  |  |  | 7,0 |
| **4** |  |  | 17 |  |  |  | 17,0 |
| **5** |  |  |  | 28,5 |  |  | 28,5 |
| **6** |  |  |  |  | 13 |  | 13,0 |
| **7** |  |  |  |  |  | 9,5 | 9,5 |
| **Итого баллов за критерий/модуль** | | 16 | 8 | 20 | 30 | 16 | 10 | 100,0 |

1.4. СПЕЦИФИКАЦИЯ ОЦЕНКИ КОМПЕТЕНЦИИ

Оценка Конкурсного задания будет основываться на критериях, указанных в таблице №3:

*Таблица №3*

**Оценка конкурсного задания**

|  |  |  |
| --- | --- | --- |
| **Критерий** | | **Методика проверки навыков в критерии** |
| **А** | Установка, конфигурирование и устранение неисправностей в корпоративных системах защиты информации | Измеряемые критерии, на основе требований, указанных в задании и критериях. Баллы начисляются (с учетом штрафов) только в случае выполнения основного функционала и задач, указанных в задании. |
| **Б** | Исследование (аудит) организации с целью защиты от угроз информационной безопасности | Субъективные (судейские) критерии, на основе требований, указанных в задании и критериях. Для высшей оценки документы должны соответствовать самым лучшим практикам документооборота, верным, непротиворечивым содержимым. |
| **В** | Политики безопасности в системе корпоративной защиты информации от внутренних угроз | Измеряемые критерии, на основе требований, указанных в задании и критериях. Баллы начисляются (с учетом штрафов) только в случае выполнения основного функционала и задач, указанных в задании. |
| **Г** | Технологии защиты и анализа сетевого трафика | Измеряемые критерии, на основе требований, указанных в задании и критериях. Баллы начисляются (с учетом штрафов) только в случае выполнения основного функционала и задач, указанных в задании. |
| **Д** | Технологии агентского мониторинга | Измеряемые критерии, на основе требований, указанных в задании и критериях. Баллы начисляются (с учетом штрафов) только в случае выполнения основного функционала и задач, указанных в задании. |
| **E** | Анализ выявленных инцидентов | Измеряемые критерии, на основе требований, указанных в задании и критериях. Баллы начисляются (с учетом штрафов) только в случае выполнения основного функционала и задач, указанных в задании. |

Существует три разных типа объективных критериев для оценки конкурсного задания. Приведенная ниже таблица описывает эти типы:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Тип** | **Пример** | **Максимальная оценка** | **Все выполнено** | **Частично выполнено** |
| Максимальный балл или ноль | Групповая политика создана, применена, выполняется на целевой машине пользователя | 0,20 | 0,20 | 0,00 |
| При уменьшении количества баллов используется скользящая шкала | Отчет отформатирован согласно спецификации  (вычесть 0,10 балла за каждую ошибку, такие как ошибки оформления, неверный выбор подписанта, смысловые ошибки и т.п.) | 0,50 | 0,50 | 0,00-0,40 |

1.5. КОНКУРСНОЕ ЗАДАНИЕ

Возрастной ценз: 18 лет и более.

Общая продолжительность Конкурсного задания[[1]](#footnote-1): 19 ч.

Количество конкурсных дней: 3 дня

Вне зависимости от количества модулей, КЗ должно включать оценку по каждому из разделов требований компетенции.

Оценка знаний участника должна проводиться через практическое выполнение Конкурсного задания. В дополнение могут учитываться требования работодателей для проверки теоретических знаний / оценки квалификации.

1.5.1. Разработка/выбор конкурсного задания

Конкурсное задание состоит из 6 модулей, включает обязательную к выполнению часть (инвариант) – 3 модуля, и вариативную часть – 3 модуля. Общее количество баллов конкурсного задания составляет 100.

Обязательная к выполнению часть (инвариант) выполняется всеми регионами без исключения на всех уровнях чемпионатов.

Количество модулей из вариативной части, выбирается регионом самостоятельно в зависимости от потребностей работодателей региона в соответствующих специалистах. В случае если ни один из модулей вариативной части не подходит под запрос работодателя конкретного региона, то вариативный (е) модуль (и) формируется регионом самостоятельно под запрос работодателя. При этом, время на выполнение модуля (ей) и количество баллов в критериях оценки по аспектам не меняются (Приложение 3. Матрица конкурсного задания).

1.5.2. Структура модулей конкурсного задания (инвариант/вариатив)

**Модуль А** **Установка, конфигурирование и устранение неисправностей в корпоративных системах защиты информации**

*Время на выполнение модуля* 4.5ч

**Задания:** Вы работаете инженером в центре информационной безопасности (департамент проектирования и внедрения) компании-интегратора DEMO Lab.

Вам поручили собрать демонстрационный стенд в отдельной «песочнице» и развернуть DLP-систему на отдельном сегменте сети.

В «песочнице» развернуты два контроллер домена (с каталогом Active Directory и ALD Pro), с которым необходимо будет осуществить интеграцию DLP-системы. До установки системы необходимо подготовить доменных пользователей.

В качестве виртуальной инфраструктуры для пилотного проекта используется среда виртуализации VMWare Workstation.

В качестве DLP-системы выбран продукт InfoWatch Traffic Monitor (IWTM). Необходимо развернуть компоненты уровня сети (network) и хоста (endpoint).

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

Необходимо использовать следующие виртуальные машины:

* **Demo.lab** (контроллер домена demo.lab)
* **ALD.Lab**  (контроллер домена aldpro.lab)
* **IWTM** (Для установки InfoWatch TrafficMonitor, Astra Linux 1.7.0)
* **IWDM** (Для установки InfoWatch DeviceMonitor, AstraLinux 1.7.3)
* **IWDD** (Для установки InfoWatch Data Discovery, AstraLinux 1.7.3)
* **Astra-cli** (ПК Astra нарушителя, AstraLinux 1.7.3)

Сетевые настройки виртуальных машин указаны в дополнительной карточке заданий.

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

В компании развернут домен со всеми сотрудниками с указанием ФИО, должности и контактов.

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

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

**Задание 1: Подготовка домена Active Directory**

Для дальнейших работ рекомендуется создать в AD подразделение организации (Organization Unit) под названием «**ROfficeAD**», добавить в него новые каталоги пользователей и компьютеров (Users и Computers). В каталог Users рекомендуется добавить следующих пользователей:

* **admin-dm** (права доменного администратора)
* **admin-db** (права доменного администратора)
* **useroffice** (права пользователя домена)
* **ldapuser** (права пользователя домена), пользователь для осуществления LDAP-синхронизации
* **tmofficer** (права пользователя домена), пользователь для входа в веб-консоль

Допускается создание дополнительных подразделений внутри указанных для удобства работы (например, для групповых политик).

Для всех пользователей необходимо задать пароль xxXX4321

**Задание 2: Подготовка домена ALD Pro**

Для дальнейших работ рекомендуется создать в создать в ALD Pro подразделение организации (Organization Unit) под названием «**ROfficeALD**», добавить в него пользователей:

* **admin-tm** (права доменного администратора)
* **useroffice-ald** (права пользователя домена)

Допускается создание дополнительных подразделений внутри указанных для удобства работы (например, для групповых политик).

Для всех пользователей необходимо задать пароль xxXX4321

**Задание 3: Настройка отношений доверия**

**Необходимо настроить двустороннее доверительное отношение между ALD Pro и Active Directory.**

В домен **ALD Pro необходимо добавить машину Astra-cli и авторизоваться в ней под пользователем useroffice из AD через отношение доверие.** Авторизация под пользователем ALDPro допустима, но оценивается меньшим количеством баллов.

**Задание 4: Настройка IWTM**

Для работы необходимо выполнить следующие настройки ВМ машины **IWTM** AstraLinux:

1. Для первоначальной установки IWTM необходимо в настройках ВМ указать объем памяти **16 ГБ. После выполнения полной процедуры установки необходимо понизить объем оперативной памяти до 8 ГБ.**
2. Выполнить настройки репозиториев, файла hosts для правильной установки IW TM.
3. Выполнить установку **IW TM** в режиме **“All in one”** с настройками по-умолчанию.
4. Настройте синхронизацию (*Зафиксировать скриншотами*):
   1. LDAP-синхронизацию (AD) для IWTM с помощью пользователя **ldapuser**.
   2. ALD Pro синхронизацию для IWTM
5. Для работы с консолью IWTM используйте доменного пользователя **tmofficer** (задать все встроенные роли (officer и administrator) и все области видимости). *Зафиксировать скриншотами*.

**Задание 5: Развертывание DLP уровня хоста. InfoWatch Device Monitor**

В соответствии с Вашей частью пилотного проекта на отдельном сегменте сети «песочницы» Заказчика необходимо развернуть следующие компоненты InfoWatch Device Monitor (IWDM) в режиме **All in one** на машину **IWDM**:

1. Для первоначальной установки IWDM необходимо в настройках ВМ указать объем памяти **8 ГБ. После выполнения полной процедуры установки необходимо понизить объем оперативной памяти до 4 ГБ.**
2. Установить базу данных PostgreSQL на машину **IWDM**
3. Установить Основной Сервер и Консоль управления на машину **IWDM**
4. Установить InfoWatch Device Monitor Client на ПК **Astra-cli** нарушителя путем **удаленного распространения** через задачи в Device. *Зафиксировать скриншотами*.
5. Выполнить синхронизации с IWTM и AD. Осуществите интеграцию сервера безопасности IWDM с Active Directory от пользователя **ldapuser**, созданного ранее. Необходимо синхронизировать каталог компьютеров и пользователей. *Зафиксировать скриншотами*.

Ваша задача — установить указанные компоненты IWDM.

**Задание 6: Развертывание InfoWatch Data Discovery**

Для контроля общих сетевых ресурсов в организации необходимо развернуть следующие сетевые компоненты InfoWatch Traffic Monitor на машину **IWDD**

1. Для первоначальной установки IWDD необходимо в настройках ВМ указать объем памяти **8 ГБ. После выполнения полной процедуры установки необходимо понизить объем оперативной памяти до 4 ГБ.**

**Задание 7: Подготовка InfoWatch Data Discovery**

После установки InfoWatch Data Discovery необходимо создать задачу на ежедневное сканирование сетевых ресурсов. Предварительно требуется создать общую сетевую папку на виртуальной машине **Demo.lab**: «share\_astra».

Необходимо настроить доступ на чтение и запись к созданной для Data Discovery сетевой папке пользователю **admin** и группе **admins** домена ALD Pro, и пользователю **useroffice** домена MS AD. Остальные пользователи доступа к папке иметь не должны

***Зафискировать скриншотом настройку прав, а также подключение к папке пользователем admin с рабочей станции AstraClient (клиент ALD Pro)***

*Зафиксировать скриншотом работоспособность data discovery и задач, проверить сработку на любой файл и любую политику. Создать отдельную выборку.*

**Задание 8: Проверочная политика**

Для проверки правильности конфигурирования IWTM необходимо создать:

1. проверочную политик на проверку на копирование, передачу, буфер обмена, хранение. В качестве объекта защиты «Проверочная политика» использовать технологию с фразой: **«Приветствуем Вас на финале!».**
2. Выполнить проверку созданной политики на все события.
3. Необходимо создать отдельную выборку на указанную политику.

*Зафиксировать скриншотом работоспособность.*

Динамичное развитие компании Demo.Lab привело к значительному расширению штата и переезду в новый офис. В связи с этим, принято решение о расширении всей ИТ-инфраструктуры компании, в том числе и систем обеспечения корпоративной безопасности.

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 имеющиеся настройки и события в системе (как IWTM, так и IWDM) необходимо сохранить при миграции.**

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

В качестве DLP-системы выбран продукт InfoWatch Traffic Monitor (IWTM). Необходимо мигрировать или развернуть с нуля компоненты уровня сети (network) и хоста (endpoint).

В соответствии с Вашей частью пилотного проекта на отдельном сегменте сети «песочницы» Заказчика необходимо мигрировать или установить с нуля на 2 разных машины следующие сетевые компоненты InfoWatch Traffic Monitor:

* Основной сервер безопасности IWTM (Node) (Astra Linux 1.7.0)
* База данных IWTM (Database) (Astra Linux 1.7.0)

Система, установленная без сохраненных событий допустима, но оценивается меньшим количеством баллов. Необходимо мигрировать Node или Database сервер на отдельную машину, которую предварительно необходимо создать самостоятельно и дать ей имя в соответствии с тем, какой компонент мигрируете – **iwtm\_db** или **iwtm\_node**. Для развертывания машины можно воспользоваться OVA образом подготовленной операционной системы Astra Linux (информация находится в дополнительной карточке).

Параметры IWTM: версия — Enterprise, СУБД — PostgreSQL.

Все развернутые сервера должны быть доступны для управления (службы) и мониторинга из консоли управления IWTM.

Ваша задача — установить указанные компоненты IWTM используя распределенный сценарий установки.

Подтвердить выполнение задания скриншотами (основные моменты: правка конфигурационных файлов, изменение настроек, проверка работоспособности, отчет о состоянии системы в web-консоли IWTM).

**Задание 9: Развертывание DLP уровня хоста. InfoWatch Device Monitor.**

В соответствии с Вашей частью пилотного проекта сети Заказчика необходимо произвести миграцию следующих endpoint-компонентов InfoWatch Device Monitor (IWDM):

* Основной сервер безопасности (Node)
* База данных IWDM-DB (Database). **Сохранение всех событий и конфигураций будет значительным плюсом.**

Версия СУБД IWDM для установки или миграции — PostgreSQL.

Необходимо мигрировать Node или Database сервер на отдельную машину, которую предварительно необходимо создать самостоятельно и дать ей имя в соответствии с тем, какой компонент мигрируете – **iwdm\_db** или **iwdm\_node**. Для развертывания машины можно воспользоваться OVA образом подготовленной операционной системы Astra Linux (информация находится в дополнительной карточке).

В случае невозможности сохранения конфигурации допускается установка с нуля. Это не будет являться полным выполнением задания, но позволит перейти к следующим этапам.

**Задание 10: Проверочная политика**

Для проверки правильности разнесения компонентов IWTM необходимо создать:

1. проверочную политик на проверку на копирование, передачу, буфер обмена, хранение.
2. Необходимо создать отдельную выборку на указанную политику.

В качестве объекта защиты необходимо использовать технологию с фразой: «Разнесение настроено успешно!»

*Зафиксировать скриншотом работоспособность.*

**Задание 11: Беспарольное SSH-соединение защищенного доступа к IWTM**

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

Парольная фраза для ключа (если применимо): xxXX1234 (или своя, поместить в файл отчета на рабочем столе), файл ключа также сохранить рядом с файлом отчета.

Зафиксируйте все этапы (генерация ключа, подключение) выполнения задания скриншотами. Необходимо сохранить SSH-сессию в SSH-клиенте для проверки

**Задание 12. Защита HTTPS-соединения с IWTM. Создание цифровых сертификатов**

Для корректной работы некоторых сервисов, предоставляемых внутри компании, заказчику необходимо развернуть структуру PKI. Сгенерированные сертификаты не должны иметь ошибок, критических полей (кроме указанных) или неверных данных. Так же после генерации всех сертификатов, они должны быть установлены в локальное хранилище на контроллере домена.

Все сертификаты и соответствующие им закрытые ключи должны быть помещены в папку на рабочем столе. Далее указана информация для сертификатов, которую они должны содержать. Можно использовать любое удобное ПО для работы с сертификатами, не допускается ошибок в основных и дополнительных полях сертификата.

**Общие свойства (поля) для всех сертификатов:**

Страна: RU  
Город: Ufa  
Область: RB  
Организация: FIRPO  
Подразделение: IT

**Корневой сертификат:**

commonName: CA  
E-mail: [ca-support@demo.lab](mailto:ca-support@demo.lab)

Период действия: 10 лет   
Альтернативные имена субъекта по DNS: CA; CA.demo.lab

**Промежуточный сертификат:**

commonName: Intermediate  
E-mail: support@demo.lab

Альтернативные имена субъекта по DNS: Intermediate; Intermediate.demo.lab

**Серверный сертификат:**

E-mail: iwtm@demo.lab

Алгоритм подписи: SHA 256   
Закрытый ключ: RSA:2048 bit   
Период действия: 365 дней

**Пользовательский сертификат (должен запрашиваться с клиентов при соединении с сервером IWTM):**

E-mail: user@demo.lab

Период действия: 365 дней

*Генерацию сертификатов зафиксируйте скриншотами.*

*Созданные сертификаты, ключи, скрипты для их создания и скриншоты процесса разместите в папке «Certificates IWTM» на рабочем столе компьютера.*

**Задание 13. Защита HTTPS-соединения с IWTM. Использование цифровых сертификатов**

Примените цифровые сертификаты для защиты клиент-серверного соединения по протоколу HTTPS при подключении к веб-консоли IWTM со всех узлов сети домена по DNS-имени вашего Traffic Monitor. Для этого необходимо установить серверный сертификат на веб-сервер Traffic Monitor, а клиентский — на устройства в сети.

Проверку необходимо осуществить с помощью браузера Google Chrome. Проверка должна производиться через всплывающее окно запроса сертификата.

*Зафиксируйте все этапы выполнения задания (настройка веб-сервера, установка защищенного HTTPS-соединения и т. п.) скриншотами.   
Необходимо указать в отчете, с помощью какого DNS имени осуществлялась проверка соединения.*

**Модуль Б. Исследование (аудит) организации с целью защиты от угроз информационной безопасности**

*Время на выполнение модуля* 3ч

**Задания:**

Вам, как специалисту, поручено **разработать  концепцию политики защиты данных** с целью реализации мер по обеспечению безопасности персональных данных  (152-ФЗ, ПП1119, Приказ ФСТЭК России №21 и другие документы). В процессе проведения аудита и формирования политики защиты персональных данных Вы должны решить следующие задачи:

1. В соответствии с  Постановлением Правительства РФ от 1 ноября 2012 г. N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" **определить уровень защищенности персональных данных** при их обработке в информационной системе организации. Решение обосновать.
2. В соответствии с Приказом ФСТЭК России N 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" **определить содержание мер по обеспечению безопасности персональных данных**, адаптируя базовый набор мер под требования решения задач *обеспечения целостности информационной системы и персональных данных (ОЦЛ).*

3.Для реализации мер *обеспечения целостности информационной системы и персональных данных*  необходимо сформировать концепцию политики защиты данных (в соответствии с шаблоном, представленном в приложении), описав:

* используемые технологии анализа,
* объекты защиты,
* списки отправителей/получателей,
* политики защиты данных,
* правила агентского мониторинга.

Концепция политики защиты данных, должна предусматривать:

* выявление фактов неправомерной передачи защищаемой информации из информационной системы через различные типы сетевых соединений, включая сети связи общего пользования и реагирование на них;
* выявление фактов неправомерной записи защищаемой информации на неучтенные съемные машинные носители информации и реагирование на них;
* выявление фактов неправомерного вывода на печать документов, содержащих защищаемую информацию и реагирование на них;
* выявление фактов неправомерного копирования защищаемой информации в прикладное программное обеспечение из буфера обмена и реагирование на них;
* контроль хранения защищаемой информации на серверах и автоматизированных рабочих местах;
* выявление фактов хранения информации на общих сетевых ресурсах (общие папки, системы документооборота, базы данных, почтовые архивы и иные ресурсы).

**Исходные данные**

Научно-исследовательская компания «Демо Лаб» (далее - Оператор) занимается контрактной разработкой и продажей перспективных электронных систем в интересах государственных и коммерческих организаций.

Компания обладает значительной клиентской базой, детальной информацией о партнёрах, заказчиках, клиентах за 10 лет работы. Клиентская база (около 2000 клиентов) составляет основу для деятельности по направлению продаж электронных компонент, но не оказывает влияния на направление системных разработок.

С точки зрения кадрового, бухгалтерского и финансового документооборота компания является типовой для Российской федерации.

Сотрудники (300 человек) могут обмениваться информацией посредством Почты/Email, мессенджеров/WhatsApp. Также у ряда сотрудников есть корпоративные сотовые телефоны, через которые также проходит обмен информацией.

ИСПДн Оператора (клиентская часть приложения, реализующая интерфейс пользователя) функционирует на базе АРМ под управлением ОС MS Windows 10 и состоит из следующих программных компонентов:

 − СУБД Microsoft SQL Server 2016;

− 1С Предприятие: Бухгалтерия (версия 8);

− 1С Зарплата и управление персоналом (версия 8);

− СБиС.

ИСПДн предназначены для автоматизации обработки информации:

− ПДн лиц, которые являются клиентами компании;

− ПДн сотрудников Оператора.

В ИСПДн одновременно обрабатываются персональные данные менее чем 100000 субъектов персональных данных. Все информационные системы Оператора, кроме ИСПДн Сбис, являются локальными информационными системами, поскольку входящие в ее состав технические средства обработки информации размещены в пределах одного здания.  В качестве среды передачи данных используется локальная сеть Оператора.

Информационная система персональных данных Оператора, функционирующая на базе АРМ специалистов кадровой службы, бухгалтерии обрабатывает следующую информацию о сотрудниках:

1. биографические сведения гражданина;
2. национальность;
3. религиозную принадлежность;
4. образование;
5. специальность;
6. занимаемую должность;
7. наличие судимостей;
8. адрес места жительства, домашний телефон;
9. состав семьи;
10. место работы;
11. размер заработной платы;
12. содержание трудового договора (контракта).

**Концепция Политики защиты данных**

## Используемые технологии анализа

## Объекты защиты

| № п/п | Название Объекта защиты | Состав объекта защиты |
| --- | --- | --- |
|  |  |  |

## Списки отправителей/получателей

| № п/п | Название периметра | Список |
| --- | --- | --- |
|  |  |  |

## Политики защиты данных

| № п/п | Название Политики | Тип политики (Политика защиты данных, Политика защиты данных на агентах) | Объекты защиты | Правила срабатывания |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |

## Правила агентского мониторинга

| № п/п | Правило | Описание правила |
| --- | --- | --- |
|  |  |  |

**Модуль В. Политики безопасности в системе корпоративной защиты информации от внутренних угроз**

*Время на выполнение модуля* 2 ч

**Задания:**

Создайте в системе InfoWatch Traffic Monitor 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 TM: категориями и терминами, технологиями, объектами защиты и т. п.

• При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием.

• Списки сотрудников, занимаемые позиции и отделы сотрудников (HR, Accounting и др.) представлены в разделе «Персоны» Infowatch Traffic Monitor по результатам LDAP-синхронизации с AD-сервером компании

• После создания всех политик будет запущен автоматический «генератор трафика», который передаст на InfoWatch Traffic Monitor поток данных, содержащих как утечки, так и легальную информацию.

• При правильной настройке политики InfoWatch Traffic Monitor должны автоматически выявить (или блокировать) и маркировать инциденты безопасности. Не должно быть ложных срабатываний, т. к. легальные события не должны маркироваться. Должны быть выявлены все инциденты безопасности.

• Необходимо пользоваться объектами защиты.

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

**Политики** — Политика XX, например «**Политика 5**». Для комбинированных политик формат: **Политика 5.1**, **Политика 5.2** 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.**

**Задание 1**

Для правильной работы системы необходимо настроить периметр компании:

Домен: demo.lab.

Группа персон: пользователи домена.

Исключить из перехвата почту генерального директора.

*Подтвердите выполнение задания скриншотами.*

**Политика 1**

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 ≈50%) как внутри компании, так и за ее пределы. Фотография котика есть в дополнительных данных.

**Вердикт:** Заблокировать ×

**Уровень нарушения:** низкий •

**Тег:** Политика 1

**Политика 2**

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 сообщения, содержащие IP-адреса версии. Так как предприимчивые выпускники «в тихую» проводят внутренние соревнования по Counter-Strike разворачивая локальные сервера внутри компании. IP – адреса могут иметь следующие конструкции:

IPv6 – адрес (например 2001:0db8:abf2:29ea:5298:ad71:2ca0:4ff1)

IPv6 – адрес + префикс (например 2001:0db8:abf2:29ea:5298:ad71:2ca0:4ff1/32)

**Из перехвата следует исключить 2001:0df7:cef7:29f7:52f7:adf7:2cf7:4ff7**

**Вердикт:** Заблокировать **×**

**Уровень нарушения:** высокий •

**Тег:** Политика 2

**Политика 3**

В связи с внедрением DLP систем в военные подразделения, возникла необходимость контроля утечки данных.

Политика должна срабатывать в случае обнаружения в документе ФИО и звания и/или наименования техники - последовательности из заглавных букв русского алфавита идущих подряд в количестве от 1-3 – от 2 до 3 цифр, пробела и от 1 до 5 цифр(количество техники)

**Вердикт:** Заблокировать **×**

**Уровень нарушения:** высокий •

**Тег:** Политика 3

**Политика 4**

Дочерняя компания «ООО Повозка» занимается транспортировкой грузов в разные города. Каждому рейсу присваивается уникальный идентификационный номер по следующему шаблону «5 букв (кириллица, любой регистр) - (знак дефиса) номер груза (от 0 до 800, исключая следующие номера: 233 и 321) / (слеш) от 1 до 4 букв (кириллица, верхний регистр) Например:АБВГД-123/Л , ЕЁЖЗИ-665/ЪГА Не должно быть срабатывания на следующие номера грузов (например: ЁЖИКА-233/ю или УФААА-321/ШАП). Необходимо контролировать передачу, а также копирование на съемные носители и печать вышеуказанных данных. Проверить работоспособность. Учтите, что особо обобщенные регулярные выражения лучше разделить на несколько текстовых объектов для оптимизации поиска.

**Вердикт:** Разрешить **√**

**Уровень нарушения:** средний •

**Тег:** Политика 4

**Политика 5**

Необходимо создать политики для отслеживания документов (передача и копирование), содержащих договор компании (договор компании.docx).

Политики должны работать следующим образом (за периметр компании):

1. Если передается только договор компании (шаблон и заполненный шаблон, до 25% изменений) – разрешать, уровень низкий, тег «Политика 5.1».

2. Если передается договор компании, в котором присутствует фамилия генерального директора, а также главного бухгалтера – разрешать, уровень средний, тег «Политика 5.2». Политика не должна срабатывать, если в документе только фамилия директора или только фамилия бухгалтера.

3. Если передается договор компании, в котором присутствует фамилия генерального директора, главного бухгалтера, а также стоит печать компании (ООО Повозка) – разрешить, уровень высокий, тег «Политика 5.3».

Проверить работоспособность. Политики не должны срабатывать внутри компании, только при передаче за периметр.

Все политики, объекты и прочие элементы должны называться в соответствии с номерами (например Объект 5.1, Политика 5.2, Технология 5.3 и т. д.)

**Вердикт 1:** Разрешить **√**

**Уровень нарушения 1:** низкий •

**Тег 1:** Политика 5.1

**Вердикт 2:** Разрешить **√**

**Уровень нарушения 2:** средний •

**Тег 2:** Политика 5.2

**Вердикт 3:** Заблокировать **×**

**Уровень нарушения 3:** высокий •

**Тег 3:** Политика 5.3

**Политика 6**

Стало известно, что сотрудники охраны (Security) ООО «Повозка» за определенную сумму пропускают автомобили из близлежащих домов на служебную парковку. В связи с ужесточением корпоративной политики в компании, правом въезда на территорию обладает только генеральный директор.

Сотрудники охраны ведут журнал учета автомобилей в электронном виде и обмениваются между собой данными о припаркованных автомобилях.

Необходимо детектировать и блокировать номера всех автомобилей, которые незаконно парковались на частной территории компании ООО «Повозка», исключая номер автомобиля генерального директора М333АО102.

Буквы, используемые в автомобильных номерах:

А, В, Е, К, М, Н, О, Р, С, Т, У, Х (Верхний регистр)

Цифры, используемые в автомобильных номерах:

000 – 999

Регионы автомобильных номеров, подлежащие детектированию:

102, 02, 702

**Вердикт:** заблокировать **×**

**Уровень нарушения:** Высокий **•**

**Тег:** Политика 6

**Политика 7**

В честь юбилея компании была запущена акция с промокодами на скидку в 50% на перевозки для постоянных клиентов. По условиям акции промокод выдается только по запросу постоянного клиента. Есть вероятность утечки промокодов, в связи с этим необходимо контролировать защитить учечку текстового документа, содержащего промокоды («коды.docx»). Стоит учесть, что сотрудники могут слить не весь файл, а один или несколько купонов. Запретить передачу данных, содержащих информацию об этих купонах, а также отслеживать копирование этой информации на внешние носители, тег «Политика 7»

Проверить работоспособность на все купоны и на 1-2 купона.

**Вердикт:** заблокировать ×

**Уровень нарушения:** средний •

**Тег:** Политика 7

**Политика 8**

В связи с тем, что компания является оператором обработки персональных данных, необходимо запретить всем сотрудникам кроме отдела кадров отправлять документы, содержащие информацию о СНИЛС, ИНН, паспортных данных (в текстовом и графическом виде) за пределы компании.

**Вердикт:** заблокировать **×**

**Уровень нарушения:** средний **•**

**Тег:** Политика 8

**Политика 9**

Два месяца назад в компании DemoLab заметили, что сотрудница отдела кадров расходует в три раза больше бумаги, чем прежде, хотя объем работ не был увеличен. Путем наблюдения за сотрудницей было установлено, что она, состоя в совете школьной родительской общественности, регулярно собирает деньги с родителей за печать докладов и рефератов учеников класса, бесплатно распечатывая их в компании.

Необходимо создать политику безопасности, которая будет включать слова (с учетом морфологии): «реферат», «доклад», «ученик», «школа», «класс».

**Вердикт:** Заблокировать ×

**Уровень нарушения:** низкий •

**Тег:** Политика 9

**Политика 10**

В последнее время сотрудники стали чаще обсуждать популярные сериалы в мессенджерах и социальных сетях, из-за чего упала общая производительность на 5%. Было решено отследить, кто больше всего занимается не рабочей деятельностью, для чего необходимо создать политику для отслеживания 5 (пяти) популярных на данный момент сериалов при передаче через веб-сообщения и почту.  
Список: Ривердэйл, Сестра Рэтчед, Племена Европы, Сквозь снег, Варвары

**Вердикт:** разрешить **√  
Уровень нарушения:** низкий **•  
Тег:** Политика 10

**Политика 11**

Служба безопасности подозревают сотрудника ИТ подразделения в передаче NTLM хэшей. Необходимо выяснить, кто из ИТ подразделения занимается передачей информации. Поставьте на контроль передачу данных только ИТ подразделения как за пределы компании, так и внутри.

**Вердикт:** Заблокировать **×  
Уровень нарушения:** средний **•   
Тег:** Политика 11

**Политика 12**

Компания-партнёр ООО «Рога» занимается разработкой технических чертежей. Необходимо запретить передачу за периметр компании

У каждого чертежа есть уникальный номер, состоящий из:

Первые 3 буквы латиница верхний регистр кроме E, D и F после идет “-“ номер от 0001 до 5000 после “+” 3 буквы кириллица или латиница верхний регистр. Если идут 3 буквы кириллица: “-“ и 3 цифры. Если латиница: “/” и 2 цифры.

Исключить серию номеров от 4 300 до 4 450 включительно.

Должны срабатывать на ART-0096+ASD/66 VBN-1386+ВАЧ–345

Не должны срабатывать на AET-0096+ASD/66 VBN-1386+ВАЧ/34

**Вердикт:** Заблокировать **×**

**Уровень нарушения:** средний **•**

**Тег:** Политика 12

**Политика 13**

У директора компании скоро юбилей и сотрудники решили его поздравить, сделав коллаж из его фотографий. Для того чтобы данное поздравление не попало к директору раньше срока, необходимо контролировать передачу фотографий директора, как внутри компании, так и за его пределами. Критичным является минимум 20%-ное совпадение передаваемого фото.

**Вердикт:** разрешить **√**

**Уровень нарушения:** низкий **•**

**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, [dobrochan.org](http://dobrochan.org/b/), [ii.yakuji.moe](http://ii.yakuji.moe/abe/)

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

**Вердикт:** разрешить **√**

**Уровень нарушения:** средний **•**

**Тег:** Политика 14

**Политика 15**

В связи с внедрением DLP систем в военные подразделения, возникла необходимость контроля утечки данных. Политика должна срабатывать в случае обнаружения в документе военного билета с номером и/или ВУС - последовательности из цифр алфавита идущих подряд в количестве 6 и букв от А-Д(категории годности)

**Вердикт**: Заблокировать **×**

**Уровень нарушения**: Средний •

**Тег**: Политика 15

**Политика 16**

Необходимо поставить на мониторинг все файлы сертификатов (DER, PKCS), так как попытки передачи таких данных несут потенциальную опасность компрометации сервисов компании.

Проверить работоспособность.

**Вердикт:** разрешить **√**

**Уровень нарушения:** средний **•**

**Тег:** Политика 16

**Модуль Г. (*Название модуля*)**

*Время на выполнение модуля* 4.5ч

**Задания:**

# Задание 1: настройка сетевого окружения и компонентов систем

С помощью технологии виртуальных машин VMWare Workstationдля выполнения задания смоделирована корпоративная сеть организации на 2 филиалах и 1 офисе партнеров.

Необходимо самостоятельно настроить соединения между виртуальными машинами используя сетевые интерфейсы.

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. Скриншоты необходимо сохранить на рабочем столе в папке «Модуль InfoTeCS». Формат названия скриншотов: ITCS-1-2-1.jpg (задание 1.2, скриншот 1). Можно добавить комментарий (ITCS-1-2-1-Coordinator).

**Делать лишние скриншоты установки ПО нет необходимости, только скриншоты работоспособности!**

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

Доступ на все Windows 10: xxXX1234 или без пароля

Все пароли пользователей в сети ViPNet сделать 12344321

Все пароли администраторов в сети ViPNet сделать xxXX1234.

**В случае изменения паролей обязательно отразить это в отчете!**

**Перед установкой ПО ViPNet необходимо настроить сеть в соответствии со схемой.**

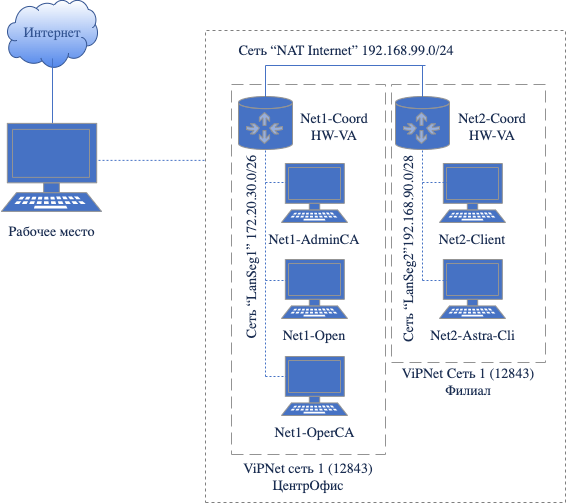
**Необходимо записать все IP адреса, логины и пароли в текстовый файл vipnet.txt на рабочем столе хост-компьютера, где развернута сеть 1.**

!

**В связи с особенностями работы системы на различных версиях Windows может потребоваться устанавливать компоненты системы вручную (например БД, сервер ЦУС, клиент ЦУС) используя пакеты MSI в подпапках дистрибутивов.**

**При выполнении задания можно пользоваться документацией к ПО, презентациями из папки и справочными ресурсами в интернете.**

Схема сети, которую требуется создать, приведена далее.

  
Рисунок 1 Схема защищенной сети

## Задание 1.1. Установка физического HW для Центрального Офиса:

Вам предоставлен физический координатор HW для Центрального офиса. Установка и настройка физического координатора будет оцениваться максимальным баллом. Установка и настройка виртуального координатора для Центрального Офиса не считается ошибкой и может быть реализовано, однако, будет оценено меньшим количеством баллов.

## Задание 1.2. Установка ПО ViPNet Administrator для создания защищённой сети:

Если были произведены изменения паролей, IP-адресов и так далее, необходимо отразить это в отчете.

* Установить базу данных MSSQL на Net1-Open (незащищенный узел)
* Установить и настроить рабочее место администратора VipNet Certification Authority (на базе виртуальной машины Net1-AdminCA (ЦО)): Центр управления сетью (**серверное приложение ЦУС**), Удостоверяющий и ключевой центр (УКЦ); использовать ранее установленную БД.
* Установить **клиент ЦУС** на ВМ Net1-Open (незащищенный узел)

Установка «Все-в-одном» будет считаться некорректным выполнением развертывания, но допустимо для продолжения дальнейшей работы.

* На компьютере на Net1-AdminCA (ЦО) установить ПО ViPNet Client (Windows), рабочее место администратора;
* Установить драйверы РуТокен, которые потребуются для дальнейшей аутентификации пользователя.

Если были произведены изменения паролей, IP-адресов и так далее, необходимо отразить это в отчете.

## Задание 1.3. Установка центра регистрации, сервиса публикации и сервиса информирования VipNet Certification Authority на соответствующие виртуальные машины:

* На компьютере на Net1-OperCA(ЦО) установить ПО ViPNet Client (Windows);
* На компьютере на Net1-OperCA(ЦО) установить ПО ViPNet Publication Service;
* На компьютере на Net1-OperCA(ЦО) установить ПО ViPNet Registration Point;
* На компьютере на Net1-AdminCA (ЦО) установить ПО ViPNet CA Informing;

**Задание 1.4. Установка ПО VipNet для организации сети филиала:**

* На ВМ Net2-Client (филиал) установить ПО ViPNet Client Windows, рабочее место пользователя;
* На ВМ Net2-Astra-Cli (филиал) установить ПО ViPNet Client Linux, рабочее место пользователя;

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

Необходимо использовать рабочее место администратора для создания структуры защищенной сети предприятия и настроить необходимые АРМ в соответствии с заданными ролями. 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 пользо-вателя узла** |
| Net1-AdminCA (ЦО) | Главный администратор (VM) | ViPNet Administrator (ЦУС сервер + УКЦ) ViPNet Client  ViPNet CA Informing | ОС Windows 10 | Admin |
| Net1-OperCA (ЦО) | Оператор УЦ | ViPNet Client  ViPNet Publication Service, ViPNet Registration Point | ОС Windows 10 | OperCA |
| Net1-Open (ЦО) | Клиент ЦУС, База данных ЦУС | Клиент ЦУС,  БД MSSQL | ОС Windows 10 | — |
| Net1-Coord  HW (ЦО) | Координатор Центр Офис (VM) | ViPNet Coordinator HW | HW-VA | CoordinatorOffice |
| Net2-Coord  HW (Филиал) | Координатор Филиал (VM) | ViPNet Coordinator HW | HW-VA | CoordinatorSub |
| Net2-Client (филиал) | Пользователь\_2 Филиал (VM) | ViPNet Client | ОС Windows 10 | User2 |
| Net2-Astra-Cli (филиал) | Пользователь\_3 Филиал (VM) | ViPNet Client | ОС Astra Linux SE | User3 |

*Связи между узлами необходимо настроить самостоятельно.*

Таблица 2. Схема связей пользователей

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Схема связей пользователей | Coord Office | Admin | OperCA | Coord Sub | User2 | User3 |
| Coord Office | × | **\*** | **\*** | **\*** |  |  |
| Admin | **\*** | × | **\*** |  | **\*** | **\*** |
| OperCA | **\*** | **\*** |  | × |  |  |
| Coord Sub | **\*** |  |  | × | **\*** | **\*** |
| User2 |  | **\*** |  | **\*** | × | **\*** |
| User3 |  | **\*** |  | **\*** | **\*** |  |

**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.  
  **Для аутентификации пользователя узла Admin использовать токен (устройство), драйверы есть на «диске» rutoken.iso:   
  Пин-код пользователя: 12345678, администратора: 87654321  
  В случае несовпадения обратитесь к экспертам.**
* 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 на рабочем столе. Сформировать дистрибутивы ключей для всех сетевых узлов (сохранить на жесткий диск). Создать группы узлов для центрального офиса (удостоверяющего центра) 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, 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**.
* Произвести первичную инициализацию HW
  + Настроить удаленный доступ через веб интерфейс к HW с открытого узла своей сети

**Необходимо проверить работоспособность сети с помощью отправки текстовых сообщений между Администратором и пользователем филиала.**

**Необходимо проверить работоспособность сети с помощью отправки деловой почты между Администратором и пользователем филиала.**

**Отправку и получение сообщений зафиксировать скриншотами.**

## Задание 2.2. Настройка работы удостоверяющего центра в аккредитованном режиме

Необходимо перевести УКЦ в режим аккредитованного удостоверяющего центра, настроить параметры издания квалифицированных сертификатов, указав:

* Сведения о средствах УЦ,
* Средство электронной подписи издателя: ViPNet CSP
* Средство удостоверяющего центра: ПК ViPNet УЦ 4
* Сертификат на средство электронной подписи издателя: Сертификат Demo.lab.crt
* Сертификат на средство удостоверяющего центра: Сертификат Demo.lab.p7b
* В настройках средства электронной подписи владельца сертификата ничего менять не требуется.
* Класс защищенности, которому соответствуют программные средства УЦ,

После перевода УКЦ в аккредитованный режим необходимо выпустить:

1. Корневой квалифицированный сертификат. Назначить текущим.
2. Квалифицированную электронную подпись для пользователя Admin. Выдать с новым дистрибутивом ключей.
3. Квалифицированную электронную подпись для пользователя Client. Сохранить электронные ключи в файл.
4. При выдаче сертификатов необходимо заполнить следующие поля:

**Имя: <Имя пользователя или узла>  
Электронная почта: <Имя пользователя>@demo.lab  
Город: Уфа  
Область: Республика Башкортостан  
Страна: RU  
Организация: ФИРПО  
Подразделение: Защита информационной безопасности  
Почтовый индекс: 123123**

Создать квалифицированные ключи ЭП и ключи проверки ЭП для пользователей сети.

Настроить схему обмена файлами между УКЦ посредством Сервиса Публикации (ViPNet Publication Service).

Настроить переход в автоматический режим (при бездействии администратора): передачу на публикацию и обновление CRL с периодичностью 1 день.

Реализовать автоматическую публикацию сертификатов издателей на FTP-сервере.

Посредством Центра Регистрации (ViPNet Registration Point):

* зарегистрировать пользователя: User4.
* Отправить запрос в УКЦ на выпуск сертификата, удовлетворить запрос. Результат выпуска сертификата зафиксировать скриншотом.
* Отправить запрос в УКЦ на аннулирование ранее выпущенного сертификата, удовлетворить запрос. Результат зафиксировать скриншотом.

Посредством Сервиса Информирования (ViPNet CA Informing):

* Сформировать отчет о выданных за текущие сутки сертификатах, предварительно в настройках указав место хранения отчетов (на рабочем столе).

## Задание 2.3. Сервер установки штампа времени и подписание OCSP.

Компании необходим сервер, отвечающий за выдачу штампов времени пользователям. Поэтому в сети филиала на узле с клиентом ViPNet должен быть установлен сервер TSP-OCSP (ПК ViPNet УЦ 4).

Для функционирования сервера необходимо издать сертификат для TSP сервиса. Поместить контейнер ключей и сертификат необходимо в программу ViPNet CSP. И после указать изданный сертификат для TSP в программе TSP-OCSP Service.

Также для корректной работы TSP сервера необходимо на работающем сервере УКЦ создать политику применения, которая будет использоваться для выдачи дальнейших сертификатов:

* Наименование: test TSP Policy
* Идентификатор: 1.2.643.100.1.2.3
* Краткое описание: Проверка штампа времени

Для TSP сервера необходимо задать эту политику применения по умолчанию.

Перед запуском TSP-OCSP сервера, требуется провести небольшую настройку:

* Номер порта сервера: 8777
* Серийный номер: 01 00 00 00 00 00 00 00
* Параметры OSCP-сервера: отключить все функции.

## Задание 2.4. 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.

Необходимо зафиксировать процесс настройки скриншотами:

* Компрометация пользователя.
* Смена ключей пользователя и сетевых узлов.
* Процедура смены ключа на клиенте с использованием резервного набора ключей.
* Скриншот экрана «защищенная сеть» в VipNet Monitor на узле Пользователь\_2 Филиал + результат проверки доступности узлов.

**Необходимо делать скриншоты до, после и в процессе компрометации, иначе другие задания могут быть не зачтены в случае неудачной компрометации.**

**Задание 2.5. Policy manager**

2.2.1 Создать шаблон политики безопасности, т. е. определить сетевой фильтр в соответствии c которым Net2-Astra-Cli должен быть доступен по SSH только с узлов Admin СА и внешней сети (фильтр защищенной сети) для работоспособности соединения с Net3-Open.

Назначить сформированный шаблон сетевым узлам, отправить политику безопасности на сетевой узел.

Зафиксировать результат (скриншотами) через журнал отправки и применения политик безопасности, на узлах в Мониторе просмотреть списки сетевых фильтров.

2.2.2 Создать шаблон политики безопасности для запрета на использование популярных соцсетей vk.com, facebook.com, tiktok.com с узлов пользователей сети (клиенты).

Применить политику к клиентам.

Зафиксировать результат (скриншотами) настройки и проверки.

2.2.3 Создать шаблон политики безопасности для возможности подключения защищенных и незащищенных узлов своей сети по протоколу RDP к AdminCA. Также необходимо включить RDP доступ на данном узле.

Применить политику к устройствам.

Зафиксировать результат (скриншотами) настройки и проверки.

**Задание 3. Межсетевое взаимодействие защищённых сетей**

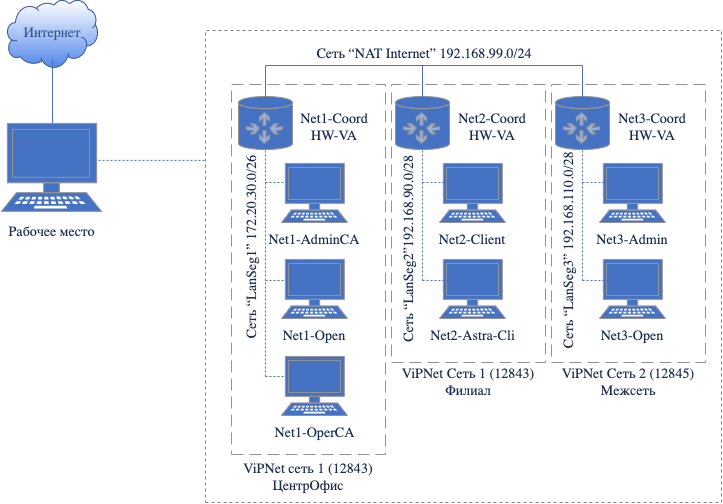


Рисунок 2 Схема межсетевого взаимодействия

Развернуть на Net3-Admin (Сеть 2 межсеть) на ПК рабочее место Администратора партнёрской сети, создать структуру второй сети:

* Рабочее место администратора (БД, ЦУС, УКЦ, ViPNet Client)
* 1 координатор HW-VA
* 1 узел Admin и пользователь Admin

Настроить связи узлов/пользователей администраторов и необходимых для работоспособности узлов.

Инициализируйте HW-VA: при настройке необходимо включить DHCP сервер

Все пароли пользователей в сети ViPNet сделать 12344321

Пароли администраторов сети ViPNet сделать xxXX1234

* Установить и настроить необходимое ПО
* Настроить межсетевое взаимодействие с использованием ассиметричных межсетевых ключей между двумя защищёнными сетями, сделать скриншоты всех этапов установки межсетевого взаимодействия.  
  **ВНИМАНИЕ!** Настройка межсетевого взаимодействия с использованием симметричных ключей не будет считаться полноценным выполнением задания
* Проверить взаимодействие узлов, отправив сообщение деловой почты в программе ViPNet Client Monitor с узла Admin (сеть 1) на Admin (сеть 2).

Необходимо предоставить:

* Файлы HTML структуры защищенной сети для обеих сетей после выполнения задания.

Скриншоты:

* Скриншоты ключевых этапов установки межсетевого взаимодействия и обработки межсетевой информации (в ЦУС и УКЦ обеих сетей).
* Структура защищенной сети в ЦУС после установления межсетевого взаимодействия (для обеих защищенных сетей) с экраном проверки доступности узлов.
* Скриншоты деловой почты на отправителе и получателе (при отправке письма).
* Скриншоты текстового сообщения на отправителе и получателе (при отправке письма).

## Задание 3.1. Настройка правил в сети

* Необходимо настроить доступ к SSH по порту 4444 с узла Net3-Open до узла Net2-Astra-Cli
* Необходимо настроить удаленное подключение по протоколу RDP между узлом Net3-Open и Net2-Client
* Необходимо настроить правило, разрешающее доступ по протоколам POP3/IMAP и POP3S/IMAPS между сетями «ЦентрОфис» и «Межсеть». Правило должно работать только в рабочие дни (пн-пт), с 8:00 до 18:00. В остальное время трафик указанных протоколов должен блокироваться.

Предоставить скриншоты создания/настройки правил и скриншоты работоспособности: RDP сессии, Подключения к SSH. Зафиксировать скриншотами создание правила для SMTP и SMTPS.

**Задание 3.2.**

* Настроить Bond интерфейс(собрать из eth1-eht2) на координаторе для балансировки и резервирования(выбрать подходящий режим)

**Задание 4. Туннелирование в рамках межсетевого взаимодействия**

* Подключить незащищенную машину в сети 3
* Для второй открытой машины использовать 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); проанализировать журналы IP-пакетов на координаторах.

Скриншоты:

* Настройка максимального количества туннелей на координаторах
* Скриншоты прохождения ICMP пакетов (ping) и любого другого трафика с незащищенного узла
* Скриншоты журнала прохождения IP-пакетов на веб-интерфейсе с установленным фильтром «Туннелирование» для проверки прохождения ICMP-пакетов и любого другого трафика с помощью туннелирования

**Задание 5. Кластер горячего резервирования**

В связи с участившимися случаями «падения» координатора межсети было принято решение добавить дополнительный координатор HW-VA в «Сеть 2 Межсеть» в дополнение к Net3-Coord HW-VA.

Для настройки необходимо самостоятельно развернуть соответствующий OVA-образ из дистрибутивов в сегмент межсети, настроить горячее резервирования и проверить работоспособность отключением одного из координаторов (система не должна прекращать работать при отключении одного из устройств от сети или питания).

Выбор IP координаторов и виртуальных адресов выбирается самостоятельно и записывается в отчет на рабочем столе.

Скриншоты:

* Развертывание нового координатора и инициализация (достаточно установку ключевой информации)
* Скриншот изменения конфигурации для кластера горячего резервирования

**Оба координатора необходимо оставить включенными!**

**Модуль Д. Технологии агентского мониторинга**

*Время на выполнение модуля* 2 ч

**Задания:** **Задание 1. Групповые политики AstraLinux:**

*Зафиксируйте все этапы настройки, создания и выполнения (срабатывание, где возможно) всех политик скриншотами!*

**Политика 1**

Настройте политику паролей согласно требованиям:

1. Минимальная длина пароля обычного пользователя должна составлять 10 символов, срок действия - 3 месяца
2. Минимальная длина пароля администраторов домена должна составлять 12 символов, срок действия - 1 месяц, пароль должен включать в себя строчные буквы, заглавные буквы, цифры и спец. символы

*Проверить работоспособность. Выполнение зафиксировать скриншотом.*

**Политика 2.1**

Создайте политику, запрещающую всем пользователям кроме администраторов домена авторизацию на контроллеры домена

*Проверить работоспособность. Выполнение зафиксировать скриншотом.*

**Политика 2.2**

Создайте политику, разрешающую всем пользователям домена авторизацию на все машины кроме контроллерова домена с использованием графической сесси (в том числе RDP!). Авторизация по ssh должна быть запрещена

*Проверить работоспособность. Выполнение зафиксировать скриншотом.*

**Политика 3**

Запретите пользователю ldapbind авторизацию на серверные и клиентские машины домена. Для запрета используйте параметры пользователя вместо политик HBAC

*Проверить работоспособность. Выполнение зафиксировать скриншотом.*

**Политика 4.1**

Создайте политику, разрешающую всем пользователям домена перезапускать службу salt-minion от имени суперпользователя

*Проверить работоспособность. Выполнение зафиксировать скриншотом.*

**Политика 4.2**

Создайте политику, разрешающую администраторам домена запускать оболочку bash от имени суперпользователя

*Проверить работоспособность. Выполнение зафиксировать скриншотом.*

**Политика 5.1**

Создайте групповую политику, запрещающую выключение и перезагрузку компьютера всем пользователям, кроме администраторов. Примените политику на компьютер Astra-Cli

*Проверить работоспособность. Выполнение зафиксировать скриншотом.*

**Политика 5.2**

Создайте групповую политику, устанавливающую темну тему рабочего стола пользователям подразделения SpbOffice. Примените политику на компьютер Astra-Cli

*Проверить работоспособность. Выполнение зафиксировать скриншотом.*

**Политика 6.1**

Задайте минимальный срок жизни kerberos-билетов 12 часов

*Проверить работоспособность. Выполнение зафиксировать скриншотом.*

**Политика 7**

Создайте пользователя gpoadmin. Выдайте пользователю следующие привелегии:

* управление установкой ОС по сети;
* управление установкой и обновлением ПО;
* администрирование службы печати;
* администрирование службы синхронизации времени;
* администрирование службы динамической настройки узла;
* администрирование службы разрешения имен;
* управление компьютерами;- управление группами компьютеров;
* управление распределением компьютеров и групп компьютеров по подразделениям;
* администрирование сайтов;
* администрирование контроллеров домена;
* управление репликацией;
* управление заданиями автоматизации.

**Подтвердите выполнение задания авторизовавшись в интефрейс ALD Pro под этим пользователем**

**Политика 8.**

Настройте уведомление об окончании действия пароля за 14 дней

**Зафискируйте создание политики скриншотов**

**Политика 9.**

Выполните удаленное подключение к рабочей станции AstraCli средствами web-интерфейса ALD Pro

**Зафиксируйте работоспособность удаленного подключения скриншотом**

**Задание 1. Настройка IWDM**

Используйте для входа в консоль IWDM доменного пользователя *admin-dm*.

Задать максимальные права пользователя на работу в консоли IWDM.

*Проверить работоспособность, зафиксировать настройку и выполнение скриншотом запущенной консоли.*

**Задание 2**

Необходимо создать новые политики (кроме политики на устройства по умолчанию),

Название: «**Отдел 1**»

Группа компьютеров: Виртуальная машина **Astra-cli**

**Правила для Отдела 1:**

**Правило 1**

Необходимо собрать статистику активности сотрудника.

*Зафиксировать настройку скриншотом.*

**Правило 2**

Необходимо разрешить копирование на съемные устройства файлов интрепретатора python, размером до 10КБ.   
*Проверить работоспособность и зафиксировать выполнение скриншотом.*

**Правило 3**

В связи с небезопасностью ftp-серверов разрешить только скачивание по протоколу ftp, загрузку файлов на сервер запретить.

*Проверить работоспособность и зафиксировать настройку и выполнение скриншотами.*

**Правило 4**

В последнее время бюджет компании стал резко падать. Подозрения пали на главного бухгалтера и отдел бухгалтерии, директор подозревает их в сговоре, с целью проведении денежных средств «мимо кассы». В связи с этим необходимо вести мониторинг слов «касса», «наличка», «обналичивание» вводимых с клавиатуры на рабочих станциях пользователей.

*Зафиксировать выполнение скриншотом (окно настройки).*

**Правило 5**

Заблокируйте доступ к CD/DVD для сотрудников.

*Зафиксировать выполнение скриншотом.*

**Правило 6**

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

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

**Правило 7**

Необходимо поставить на контроль буфер обмена в текстовых процессорах (Kate).   
*Зафиксировать настройку скриншотом.*

**Правило 8**

1. Необходимо отслеживать копирование всех файлов на USB-накопители.

2. Запретить копирование файлов в ранее созданную общую папку data discovery share-astra

*Проверить работоспособность и зафиксировать выполнение.*

**Правило 9**

В связи с подозрениями необходимо делать снимки экрана пользователя каждые 80 секунд.

*Зафиксировать настройку скриншотом.*

**Модуль Е: Анализ выявленных инцидентов**

*Время на выполнение модуля* 1.5 ч

**Задания:**

**Задание 1. Пользователь**

Необходимо создать пользователя системы с правами доступа только на чтение и выполнение отчетов, сводок и событий.

* Логин: reportsuser, пароль: XxXx5467

**Задание 2: Сводки**

Создайте новые вкладки сводки в разделе «Сводка» под названием «РЧ2024» и «Особые сводки РЧ»

**Задание 2: Виджеты**

При создании выборок для сводок необходимо помещать их в каталог выборок «РЧ2024». Создайте в сводке «РЧ2024» 4 виджета:

1. Выборка по событиям data discovery за последнюю неделю
2. Выборка по политикам с технологиями: графические объекты, печати, эталонные документы за последние 3 дня
3. Статистика по политикам за последние 7 дней
4. Топ нарушителей за последние 3 дня

Неверный срок действия виджета или подборка данных для визуализации является грубой ошибкой.

**Задание 3**

Необходимо создать виджет в разделе «Сводка», вкладка «Особые сводки», отображающий события с уровнем угрозы от низкого до высокого на правила копирования и хранения за последние 7 дней.

*Зафиксировать скриншотом конструктора выборки.*

**Задание 4**

Необходимо создать виджет в разделе «Сводка», вкладка «Особые сводки» для отображения нарушений только от обоих компьютеров нарушителей (виртуальных машин) со средним и высоким уровнем угрозы за последние 3 дня.

*Зафиксировать скриншотом конструктора выборки.*

**Задание 5**

Необходимо создать виджет в разделе «Сводка», вкладка «Особые сводки» для отображения нарушений с любым тегом только от пользователей домена Demo за последний месяц.

*Зафиксировать скриншотом конструктора выборки.*

**Работа с IDS/TIAS**

**Введение**

Необходимо установить, настроить и проверить работоспособность ключевых

элементов SOC: СОВ ViPNet IDS VA, SIEM ViPNet TIAS.

Задание включает проверку на обнаружение известных атак (сгенерированных участником), так и неизвестных участнику (трафик отправляется Главным экспертом). На момент отправки трафика (моделирования угрозы/атаки)

инфраструктура выявления угроз участника в виде установленных и корректно

настроенных IDS+TIAS должна быть полностью готова. Главный эксперт

отправляет трафик по запросу до 2 раз.

Все действия необходимо документировать скриншотами в формате: IDS-2-1-3, где T — Task (задача), 1 — номер задания, 2 — подпункт задания (при наличии),

3 — шаг.

На каждое задание ОБЯЗАТЕЛЬНО необходимо сохранять скриншоты всех

действий по изменению настроек (установка, использование конструктора

фильтров, создание отчетов и т. д.) и проверке работоспособности системы и

правил. Формат скриншотов для документирования действий указан выше.

ВАЖНО! Запрещается воздействовать на инфраструктуру чемпионата, объекты

информатизации на площадки и за пределами площадки, машины других

участников и экспертов. Объектами атак при моделировании угроз должны

быть только собственные виртуальные машины.

При выполнении заданий рекомендуется использовать следующие виртуальные

машины: IDS-NS-VA, Vipnet\_TIAS, незащищенные машины OWASP, metasploitable,

дистрибутивы для тестирования (Kali, Parrot и др.) или иные свободные утилиты

и ОС.

Задание 1. Начальная установка и настройка систем ViPNet IDS VA и TIAS

1. Образ ViPNet IDS VA необходимо развернуть в VMWare ESXi.

a. Использовать 1 сетевой интерфейс для управления, 2 — для

перехвата трафика (в общей сети NAT)

b. Настроить нового администратора системы с полным доступом

(officer).

c. Настроить сетевые интерфейсы управления и перехвата,

используя карточку доп. сведений.

d. Загрузить и применить актуальные сигнатуры.

2. ViPNet TIAS необходимо развернуть в VMWare Workstation.

a. Подключить установленный ранее IDS VA в качестве сенсора.

b. Настроить нового администратора системы с полным доступом

(officer).

Зафиксировать выполнение задания скриншотами: настройка сетей,

пользователей.

Записать все логины и пароли в файле IDS.txt на рабочем столе!

Задание 2. Базовая работа с правилами ViPNet IDS VA

1. Создать и применить пользовательское правило ViPNet IDS VA

обнаружения попыток доступа к сетевым папкам виртуальной машины

(win). Проверить выполнение с помощью виртуальной машины.

2. Провести детектирование трафика согласно указанным правилам с

помощью IDS

Зафиксировать выполнение задания (правила и обнаруженные события в IDS)

скриншотами.

Задание 3 Проверка системы на выявление известной атаки: IDS+TIAS

1. Самостоятельно, с помощью утилит Kali Linux или аналогичных

имитировать атаку (на выбор) на любую виртуальную машину или иной

сетевой трафик

2. Зафиксировать детектирование атаки с помощью IDS-VA: вкладка События

3. Зафиксировать детектирование атаки с помощью TIAS: вкладки События и

Инциденты

4. Подготовить отчет об обнаруженной атаке согласно прилагаемому в

дополнительных файлах шаблону, назвать Отчет об известной атаке.docx

Зафиксировать выполнение задания скриншотами. Разместить отчет на

Рабочем столе компьютера.

Задание 5. Формирование отчетов

1. Сформировать отчет в IDS/TIAS по событиям из задания 3 (параметры

на выбор)

Все отчеты зафиксировать скриншотами..

2. СПЕЦИАЛЬНЫЕ ПРАВИЛА КОМПЕТЕНЦИИ*[[2]](#footnote-2)*

2.1. Личный инструмент конкурсанта

В компетенции не задействовано оборудование/материалы участников, инструментальный ящик, отсутствует. Участникам разрешено использовать беруши и активные наушники для защиты слуха. Активные наушники можно использовать, только если участники докажут, что они не подключены к источнику аудиосигнала.

Участники могут пользоваться ресурсами сети Интернет (если иное не запрещено Главным экспертом).

2.2. Материалы, оборудование и инструменты, запрещенные на площадке

Разрешены материалы и оборудование, перечисленные в пункте 2.1

Прослушивать музыку во время выполнения задания запрещено.

Использование сотовых телефонов, смарт часов и средств связи (за исключением представленных в инфраструктурном листе) на время выполнения задания на площадке запрещено.

3. Приложения

Приложение №1 Инструкция по заполнению матрицы конкурсного задания

Приложение №2 Матрица конкурсного задания

Приложение №3 Инфраструктурный лист

Приложение №4 Критерии оценки

Приложение №5 План застройки

Приложение №6 Инструкция по охране труда и технике безопасности по компетенции «КОРПОРАТИВНАЯ ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ».

1. *Указывается суммарное время на выполнение всех модулей КЗ одним конкурсантом.* [↑](#footnote-ref-1)
2. *Указываются особенности компетенции, которые относятся ко всем возрастным категориям и чемпионатным линейкам без исключения.* [↑](#footnote-ref-2)