

# КОНКУРСНОЕ ЗАДАНИЕ

***ДЛЯ МУНИЦИПАЛЬНОГО ЧЕМПИОНАТОВ***

***чемпионатного цикла 2024/2025***

# компетенции

«КОРПОРАТИВНАЯ ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

**для основной возрастной категории**

**14-16 года**

*Конкурсное задание включает в себя следующие разделы:*

1. [Форма участия в конкурсе](#_bookmark0) [2](#_bookmark0)
2. [Общее время на выполнение задания](#_bookmark1) [2](#_bookmark1)
3. [Задание для конкурса](#_bookmark2) [2](#_bookmark2)
4. [Модули задания и необходимое время](#_bookmark3) [3](#_bookmark3)
5. [Критерии оценки](#_bookmark4) [11](#_bookmark4)
   1. **Форма участия в конкурсе**: Индивидуальный конкурс

# Общее время на выполнение задания: 4 ч.

# Задание для конкурса

Содержанием конкурсного задания являются применение на практике систем корпоративной защиты от внутренних угроз. Участники соревнований получают описание модели организации, включая описание её организационной структуры, информации, циркулирующей внутри периметра безопасности, информационной инфраструктуры, каналов связи, видов трафика, списков пользователей.

Конкурсное задание имеет несколько модулей, выполняемых последовательно.

Конкурс включает разработку и применение политик информационной безопасности, контроль информационных потоков, анализ выявленных инцидентов и подготовку отчётов.

Окончательные аспекты критериев оценки уточняются членами жюри. Оценка производится как в отношении работы модулей, так и в отношении процесса выполнения конкурсной работы. Если участник конкурса не выполняет требования техники безопасности, конфликтен, не владеет техниками управления стрессом и разрешения конфликтных ситуаций, подвергает опасности себя или других конкурсантов, такой участник может быть отстранен от конкурса.

Время и детали конкурсного задания в зависимости от конкурсных условий могут быть изменены членами жюри.

Конкурсное задание должно выполняться помодульно. Оценка также происходит от модуля к модулю.

Если участник закончил выполнение модуля досрочно, он должен расписаться в ведомости времени напротив соответствующей информационной записи «Участник № закончил выполнение модуля».

# Модули задания и необходимое время

Таблица 1.

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование модуля** | | **Соревновательный день (С1, С2, С3)** | **Время на задание** |
| **А** | Разработка политик безопасности в системе  корпоративной защиты информации от внутренних угроз | С1 | 1 час |
| **В** | Технологии защиты и анализа сетевого трафика | С1 | 1 час |
| **С** | Технологии защиты узла и агентского мониторинга | С2 | 2 часа |

## Модули с описанием работ

**Модуль A: Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз.**

Технологии этого модуля: DLP-система, корпоративная система защиты информации от внутренних угроз

Время на выполнение: 1 час

## Пример 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.
* Некоторые политики должны быть созданы с нуля, некоторые могут быть сделаны путём модификации существующих в системе.
* Для некоторых политик необходима работа с разными разделами консоли управления TM: категориями и терминами, технологиями, объектами защиты и т. п. Способ, которым создана корректная политика, оставлен на усмотрение самого экзаменуемого.
* При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием (если в задании это не указано явно, участник должен самостоятельно задать уровень угрозы при разработке политики).
* 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 как вредоносные. Не должно быть неправильной маркировки. Должны быть выявлены все инциденты безопасности.
* Внимание! Необходимо называть политики/объекты/категории и прочие объекты в соответствии с номером и названием задания, например «Задание 1», «Политика 4», «Политика 10», «Объект 1». Без верно названных объектов проверка вашего задания может стать невозможной. При выполнении задания учитывайте, что совместно с созданными могут срабатывать стандартные политики, что необходимо предотвратить.
* В комплексных заданиях необходимо пользоваться объектами защиты.
* Задания можно выполнять в любом порядке.
* Проверьте синхронизацию времени на всех системах, т. к. расхождение во времени между системами может повлиять на актуальность событий.
* Для некоторых политик могут понадобиться дополнительные файлы, которые можно найти в папке «Additional files» в общей папке из дополнительных сведений.
* Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). В этом случае необходимо протоколировать свои результаты с помощью двух скриншотов для каждого задания (скриншот заданной политики и скриншот ее работы). Для некоторых заданий необходимо после фиксации результатов в виде скриншотов удалить заданную политику, что будет оговорено отдельно в тексте задания.
* Все скриншоты необходимо сохранить на рабочем столе в папке. Формат названия скриншотов политик:

Пример 1 для сохранения скриншота созданной политики: CP-1.jpg где СP – сокращение от англ. сreating а policy,

1 – номер задания

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

1 – номер задания.

Пример 3 для сохранения нескольких скриншотов одной работающей политики:

PW-1-2.jpg

где PW – сокращение от англ. policy work,

1. – номер задания;
2. – номер скриншота для задания 1.

При проверке политик стоит учитывать, что нарушителем могут являться не только указанные в задании пользователи, а еще и виртуальная машина с агентом мониторинга (для проверки сработки политик). Необходимо учитывать данное условие при разработке и проверке политик.

## Задание 1

Создайте локальную группу пользователей «Подозрительные» в Traffic Monitor. Добавьте в нее пользователя домена виртуальной клиентской машины.

Подтвердите выполнение задания скриншотами.

## Задание 2

Для работы системы необходимо настроить периметр компании:

* Почтовый домен: demo.lab.
* Список веб ресурсов (необходимо создать новый список ресурсов, назвав его

«Доверенные домены»): worldskills.moscow, worldskills.ru, new.guap.ru.

* Необходимо создать новый список ресурсов, назвав его «Доверенные».
* Группа персон: пользователи домена.
* Исключить из перехвата почту генерального директора. Подтвердите выполнение задания скриншотами.

## 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.

Логин: newauditor, пароль: xxXX1234

Подтвердите выполнение задания скриншотами настройки прав пользователя.

## Задание 4

В связи с постоянными проблемами при организации очередного чемпионата, совет директоров решил контролировать передачу информации о WorldSkills и межвузовском чемпионате за пределы компании. 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», «Региональные» и «Reg2021».

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

Skills», «Reg 2021». Ложных срабатываний быть не должно (например, просто на Рег или Skills).

Вердикт: разрешить Уровень нарушения: низкий Тег: Политика 4

Проверить работоспособность.

## Модуль B: Технологии защиты и анализа сетевого трафика.

Технологии этого модуля: технологии защиты сетевого трафика VPN VipNET, PKI-системы (ViPNet УЦ, Publication Service и др.)

Время на выполнение: 1 час

## Пример задания

Задание 1.1. Установка ПО ViPNet Administrator для создания защищённой

сети:

* Установить и настроить рабочее место администратора VipNet: центр управления сетью (серверное и клиентское приложение ЦУС), Удостоверяющий и ключевой центр (УКЦ).

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

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;

Необходим скриншот первого запуска приложения.

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 ниже.



INTERNET

192.168.13**X**.253/24

(**X** = Рабочее место)

**Net2**

**Net1** Офис филиал «Сеть 2 Филиал»

Главный офис «Сеть 1 ЦО»

Net1\_Lan 10.14.0.0/24

INTRANET

60.80.10.0/24

Net2\_Lan

192.168.100.0/24

Главный администратор

Net1-Admin

Координатор

Центр. офис

Net1-Coord

Координатор

филиал

Net2-Coord

Клиент ViPNet

Net2-Client

Коммутатор

Незащищенный узел

Net1-DB-Open

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 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Вирт. машина | Название сетевого узла | ПО VipNet | ОС  сетевого узла | Имя пользователя сетевого узла, уровень полномочий |
| Net2-Coord (Филиал) | Координатор Филиал (VM) | ViPNet Coordinator | ОС  Windows 10 | CoordinatorSub |
| Net2-Client (филиал) | Пользователь\_2 Филиал  (VM) | ViPNet Client | ОС  Windows 10 | User2 |

*Связи между узлами необходимо настроить самостоятельно.*

Таблица 2. Схема связей пользователей

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Схема связей пользователей** | **Coordinator Office** | **Admin** | **Coordinator Subsidiary** | **User2** |
| **CoordinatorOffice** | × | **\*** | **\*** |  |
| **Admin** | **\*** | × |  | **\*** |
| **CoordinatorSub** | **\*** |  | × | **\*** |
| **User2** |  | **\*** | **\*** | × |

**Модуль C: Технологии защиты узла и агентского мониторинга Технологии этого модуля:** Агентский монитор DLP, средства защиты узла,

групповые политики ОС Active Directory Время на выполнение: 2 часа **Пример задания**

Задания выполняются с помощью компонентов DLP системы InfoWatch.

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

Необходимо убедиться в корректном отображении результата в сводках событий.

Называйте созданные вами разделы/политики/группы и т. д. в соответствии с заданием, например «Политика 1» или «Политика 1-2» и т. д.

Для некоторых политик могут понадобиться дополнительные файлы, которые можно найти на диске “D” хост-машины.

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

Все скриншоты необходимо сохранить на рабочем столе в папке

«Модуль 5».

Формат названия скриншотов политик:

Пример 1 для сохранения скриншота созданной политики: CP-1.jpg где СP – сокращение от англ. сreating а policy,

1 – номер задания

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

1 – номер задания.

Пример 3 для сохранения нескольких скриншотов одной работающей политики:

PW-1-2.jpg

где PW – сокращение от англ. policy work,

1. – номер задания;
2. – номер скриншота для задания 1.

## Задание 1

Необходимо установить (сменить) пароль для удаления Device Monitor Agent всех виртуальных машин нарушителей с помощью средств DeviceMonitor Server (удаленно). Пароль: xxXX1357.

Проверить работоспособность и зафиксировать выполнение скриншотом

## Задание 2

Необходимо создать новую политику (кроме политики на устройства по умолчанию), назвав ее «Региональные2021», применить ее к группе компьютеров по умолчанию.

Последующие правила по заданиям должны быть добавлены в эту политику. Зафиксировать выполнение скриншотом.

## Задание 3

Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления IWDM на хост-машину (компьютер с виртуальными машинами) для удаленного доступа к серверу IWDM.

Проверить работоспособность, зафиксировать выполнение скриншотом запущенной консоли на хост-машине.

## Задание 4

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

Проверить работоспособность и зафиксировать выполнение скриншотом.

## Пример заданий на групповые политики Групповая политика 1:

С помощью редактора групповой политики запретить доступ к реестру.

Выполнение задания подтвердить скриншотами.

## Групповая политика 2:

Защита RDP-сессии с помощью SSL/TLS. создайте групповую политику, которая будет применять шифрование при подключении по RDP. Выполнение задания подтвердить скриншотами.

## Групповая политика 3:

С помощью редактора групповой политики, Настройте запрет установки программ для пользователей. Выполнение задания подтвердить скриншотами.

# 

# Критерии оценки

Таблица 2.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Критерий** | | | | **Баллы** | | |
| **Судейские аспекты** | **Объективная оценка** | **Общая оценка** |
| **D** | Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз | | | 1 | 10,00 | 11,00 |
| **E** | Технологии трафика | анализа | и защиты сетевого | 1 | 15,00 | 16,00 |
| **F** | Технологии мониторинга | защиты | узла и агентского | 1 | 7,00 | 8,00 |
| **Итого** | | | | 3 | 32 | 35 |