КОНКУРСНОЕ ЗАДАНИЕ КОМПЕТЕНЦИИ «КОРПОРАТИВНАЯ ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

2023 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:

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

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 / техников 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 ИБ»

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 угроз) 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		**А**	**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.
Е	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: 16–22 года.

Общая продолжительность Конкурсного задания[1]: 21 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 (https://disk.yandex.ru/d/Ch83p3LytLyTKA)

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 материальных возможностей площадки соревнований и потребностей работодателей региона в соответствующих

[1] *Указывается суммарное время на выполнение всех модулей КЗ одним конкурсантом.*

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.

Таблица №4

Матрица конкурсного задания

Обобщенная трудовая функция	Трудовая функция	Нормативный документ/ЗУН	Модуль	Константа/вариатив	ИЛ	КО
1	2	3	4	5	6	7

Инструкция по заполнению матрицы конкурсного задания **(Приложение № 1)**

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: 3-5 часов.

Задания: участник должен:

- Провести конфигурацию сетевой инфраструктуры (в т.ч. с использованием российских защищенных ОС, таких как Astra Linux): настроить хост-машину, сетевое окружение, виртуальные машины, и т.п.;
- Установить и настроить систему корпоративной защиты от внутренних угроз;
- Установить и настроить другие накладные СЗИ согласно заданию;
- Провести конфигурирование систем;
- Запустить систему(ы), проверить функциональность и соответствие настроек целевой сетевой инфраструктуре
- Провести имитацию процесса утечки конфиденциальной информации в системе;
- Устранить проблемы при появлении;
- Продемонстрировать работоспособность системы;
- Диагностировать возможные неисправности (согласно заданию);
- Подготовить отчёт по оценке работоспособности системы;

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

Время на выполнение модуля: 3-4 часа.

Задания: участник должен провести обследование и анализ структуры организации (как главного объекта защиты) на основании представленных материалов и стенда, её вычислительно-сетевой инфраструктуры, определить потоки данных, потенциальные угрозы и каналы утечек. Необходимо подготовить пакет документации исходя из задания.

Участник готовит отчёт, суммирующий итоги работы по Модулю. По окончании проверки участник ставит подпись в отчёте и сообщает о готовности экспертам. Эксперт фиксирует время готовности на отчёте и в протоколе.

Модуль Б считается выполненным участником при условии подписанного отчета, устного доклада участника об окончании работ.

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

Время на выполнение модуля: 3-4 часа.

Задания: цель участника – разработать политики информационной безопасности, используя инструментарий автоматизированной системы IWTM 6 и успешно их применить для выявления и/или блокирования инцидентов безопасности. Для создания инцидентов и других событий в IWTM используется специальное программное обеспечение – специальный Генератор трафика и инцидентов.

Время на выполнение модуля: 3-5 часов.

Участнику необходимо:

- Разработать новые и/или модифицировать существующие политики безопасности, перекрывающие каналы передачи данных и возможные инциденты согласно конкурсного задания;
- Занести политики информационной безопасности в DLP-систему;
- Разработать и/или модифицировать существующие объекты защиты, категории, технологии защиты в DLP-системе и т.п.;
- Применить политики для контроля трафика, выявления и/или блокирования инцидентов безопасности, создаваемых внешним Генератором трафика и инцидентов. Максимизировать число выявленных инцидентов безопасности;
- Продемонстрировать владение технологиями и умение работать с интерфейсом управления системы корпоративной защиты информации IWTM.

Участнику необходимо применить политики информационной безопасности в системе IWTM, автоматически выполнить поиск инцидентов информационной безопасности, внесенных членами жюри (с использованием стенда и Генератора трафика и инцидентов). Политики можно модифицировать, с целью выявления максимального числа инцидентов и утечек. Необходимо использовать весь набор технологий поиска и выявления уязвимостей, доступный в системе корпоративной защиты. В число инцидентов могут входить, например:

- передача персональных данных сотрудников и контрагентов по электронной почте;
- передача базы клиентов организации в архиве с использованием файловых протоколов;
- нецензурная лексика сотрудников в переписке с контрагентами;
- передача информации, составляющей коммерческую тайну и др.

Задание выполняется с помощью программного обеспечения DLP (Data Leaks Prevention) IWTM 7.x.

Примерный алгоритм выполнения на примере инцидентов и политик (на примере PCI DSS):

1. Запустить систему IWTM,
2. Ознакомиться с виртуальной инфраструктурой (стендом), используемым для выполнения заданий. Типовая инфраструктура, обычно включает:
    a. IWTM-сервер;
    b. IWDM-сервер агентского мониторинга;
    c. 1 или более виртуальных машин нарушителей;
    d. 1 или более виртуальных машин для развёртывания отдельных компонент системы (БД, консолей и т.п.);
    e. Контроллер домена (служба каталога) — AD, ALD Pro и т.п.
3. Проверить функциональность и соответствие настроек целевой сетевой инфраструктуре
4. Изучить предоставляемые материалы, используемые при создании политики ИБ в системе IWTM: концепция политики ИБ PCI DSS;
5. В консоли IWTM 7 создать объекты защиты и политику ИБ, используя технологии анализа, обозначенные в политике PCI DSS.
6. Провести проверку агента, установленного на рабочей станции «нарушитель», на предмет соединения с сервером DM.
7. В консоли DM провести проверку соединения сервера IWTM 6 с сервером IWDM, а также актуальность последней версии конфигурации IWTM 6.

a. Провести имитацию процесса утечки конфиденциальной информации. Вручную с рабочей станции «Нарушитель»

8. После окончания выполнения модуля Главный эксперт направляет поток трафика на машины участников с помощью специального Генератора инцидентов, имитирующие события ИБ, выявляемые IWTM
9. В консоли IWTM и/или IWDM автоматически получить информацию о факте утечки конфиденциальной информации. Инцидент должен быть автоматически выявлен и помечен как уязвимость соответствующего уровня согласно заданию. Не должно быть ложных срабатываний: события, не удовлетворяющие политикам DLP, не должны быть помечены как вредоносные (инциденты)

Модуль Г. Технологии защиты и анализа сетевого трафика

Время на выполнение модуля: 4-5 часов.

Задания: Участник выполняет следующие действия с использованием VPN-систем корпоративного класса (Virtual Private Network):

- Развёртывание, настройка и проверка работоспособности VPN-сети на существующей и вычислительной инфраструктуре.
- Администрирование узлов и пользователей.
- Выполнение компрометации узлов, ключей, пользователей. Восстановление связи. Обновление ключевой информации.
- Организацию межсетевого взаимодействия и туннелированния.
- Внедрение централизованных политик безопасности. Обеспечение защиты рабочих мест.

Участник выполняет следующие действия с использованием IDS/IPS/FW/NGWF-систем корпоративного класса:

- Развёртывание, настройка и проверка работоспособности СЗИ на существующей и вычислительной инфраструктуре. Настройка и подготовка инфраструктуры.
- Выявление инцидентов безопасности за ограниченное время и/или с учётом неожиданно меняющихся условий.
- Разработка и применение различных механизмов и технологий анализа трафика.
- Детектирование атак и угроз, проведение расследования инцидента

VPN и IDS системы могут применяться в рамках одного модуля как совместно, по отдельности или поодиночке.

Модуль Д. Технологии агентского мониторинга

Время на выполнение модуля: 2-3 часа.

Задания: Задача участника:

- Продемонстрировать знание механизмов работы агентского мониторинга;
- Разработать и применить политики агентского мониторинга для работы с носителями и устройствами;
- Разработать и применить политики агентского мониторинга для работы с файлами;
- Работа с исключениями из перехвата;
- Защита узлов. файерволы и т.п.;
- Групповые политики AD.

Модуль Е. Анализ выявленных инцидентов

Время на выполнение модуля: 2-4 часа.

Задания: Задача участника – использовать аналитический функционал систем корпоративной защиты от внутренних угроз, систем обнаружения вторжений (IDS/IPS), систем управления инцидентами информационной безопасности (SIEM) и др. СЗИ для создания отчётов о найденных инцидентах (в т.ч. автоматических), анализа полученных данных, получение по итогам анализа новой информации.

2. СПЕЦИАЛЬНЫЕ ПРАВИЛА КОМПЕТЕНЦИИ[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.

2.3. Использование методов и инструментов генерации трафика

Для объективного контроля функциональности и работоспособности политик безопасности в DLP-системе, разработанных участником при выполнении Модуля В необходимо использовать специальные генераторы трафика, эмулирующие (или имитирующие) наступление событий в DLP-системе: утечки данных различного вида, наличие «белого трафика» и т.п. Сценарии для генератора должны быть разработаны заранее, до дня проведения соответствующего модуля Соревнований. Стандартным подходом является запуск генератора после окончания модуля, для объективной проверки созданных участниками политик.

[2] *Указываются особенности компетенции, которые относятся ко всем возрастным категориям и чемпионатным линейкам без исключения.*

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».