ОПИСАНИЕ КОМПЕТЕНЦИИ

«КОРПОРАТИВНАЯ ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Наименование компетенции: «Корпоративная защита от внутренних угроз информационной безопасности»
Формат участия в соревновании: индивидуальный

Описание компетенции.

Обеспечение информационной безопасности является неотъемлемой частью деятельности организации. Состояние информационной безопасности представляет собой умение и способность компании надежно противостоять любым попыткам нанести ущерб её законным интересам, защищать себя от внутренних и внешних угроз.

Компетенция нацелена на защиту от внешних атак и внутренних утечек данных, произошедших умышленно или по неосторожности через технические каналы связи.

Цель компетенции – агрегация передовой теории и практики корпоративной информационной безопасности, передача экспертизы в национальную систему образования, построение и развитие профессионального сообщества.

Конкурсное задание построено на реальных сценариях применения и включает реализацию комплекса профессиональных мер по защите организаций от угроз информационной безопасности с использованием технологий Data Leakage Prevention (DLP), Intrusion Detection Systems (IDS/IPS), Virtual Private Networks (VPN), SIEM, WAF, Endpoint Security.

Одна из главных угроз корпоративной информационной безопасности – неправомерными действиями сотрудников (т.н. инсайдеров), приводящие к потере конфиденциальных данных, совершенные как целенаправленно, так и из-за халатности, невнимательности или незнания элементарных правил безопасности предприятия. Именно «на их совести» большинство громких краж данных, зафиксированных по всему миру в последние годы. Причиной утечек также могут быть действия посторонних лиц, находящихся на территории предприятия и имеющих доступ к вычислительно-сетевой инфраструктуре (клиенты, поставщики и т.п.).

Неотъемлемой частью работ по обеспечению корпоративной безопасности от внутренних утечек является проведение всего комплекса

технических мероприятий по анализу потоков данных, как циркулирующих внутри периметра защищаемой информационной системы, так и пересекающих его. Для этого специалисты должны уметь проводить весь цикл работ по установке, развёртыванию, настройке, использованию DLP-систем, включая разработку политик информационной безопасности, классификацию объектов защиты, применение технологий фильтрации различных видов трафика, фильтрацию перехваченного трафика для поиска найденных инцидентов, выдачу разрешения/запрещения на доставку определенных данных, анализ содержимого перехваченного трафика с целью выявления нарушений корпоративной политики безопасности, диагностику работоспособности, и т.п.

Важным направлением обеспечения безопасности корпоративной информации – реализация прозрачного доступа к территориально-распределенным информационным ресурсам компании через сети связи общего пользования, в том числе Интернет. Для защиты передаваемых данных используется технологии виртуальной частной сети (Virtual Private Network, VPN) и межсетевого экранирования, включая защиту информации, передаваемой по каналам связи; защиту сети в целом, ее сегментов от несанкционированного доступа, как из внешних, так и из внутренних сетей; контроль трафика между узлами VPN-сети, включая фильтрацию трафика; использование в качестве транспортной среды передачи данных каналы сетей связи общего пользования; возможность модернизации, модульного наращивания VPN-сети; централизованное управление VPN-сетью.

Для предотвращения и минимизации последствий атак на корпоративную инфраструктуру и объекты защиты, необходимо их своевременное выявление и правильная классификация с использованием систем обнаружения атак IDS/IPS (Intrusion Detection/Prevention System), межсетевых экранов (в т.ч. промышленного класса, с использованием технологий DPI), файрволов уровня приложений и т.п.

Специалисту по корпоративной защите от угроз информационной безопасности необходимо знать и уметь применять на практике средства защиты информации и механизмы разграничения доступа операционных систем, такие как групповые политики корпоративного сетевого каталога (домена), модели контроля и управления доступом, цифровые сертификаты, элементы инфраструктуры открытых ключей (PKI), системы контроля целостности, системы защиты узла и т.п.

Помимо перечисленного, специалист по корпоративной безопасности должен уметь подготовить отчёты о найденных инцидентах (с оценкой уровня угрозы и нормативной оценкой) менеджменту организации, которую

защищает, а также правильно оценить угрозы и риски информационной безопасности.

Актуальность профессии (специальности) в реальном секторе экономики России определяется многократным ростом угроз, кибератак, а увеличением числа утечек критической для деятельности российских организаций данных.

Особенностью профессиональной деятельности специалиста в области корпоративной защиты от внутренних угроз ИБ является комплексное понимание вопросов защиты информации, потенциальных угроз, актуальных рисков, векторов атак и возможностей средств защиты информации, используемых для борьбы с ними.

Задачи профессиональной деятельности специалиста по защите от внутренних угроз информационной безопасности, включают:

- Обследование объекта защиты, анализ выявленных нарушений, уязвимостей
- Установка и конфигурирование корпоративной системы защиты информации от внутренних угроз ИБ
- Установка и конфигурирование корпоративных СЗИ
- Проведение диагностики, выявление и устранение неисправностей
- Исследование (аудит) организации с целью защиты от угроз информационной безопасности
- Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз
- Эксплуатация и администрирование СЗИ, в т.ч. корпоративной системы защиты информации от внутренних угроз ИБ
- Применение на практике технологий защиты и анализа сетевого трафика
- Применение на практике технологий агентского мониторинга
- Анализ выявленных инцидентов
- Подготовка отчетов
- Подготовка пакета документов по итогам расследования для принятия кадровых решений и/или обращения в правоохранительные органы
- Подготовка документации и внутренних нормативных документов организации
- Анализ требований стандартов, указаний регулятора регулятора, законодательства применительно к сфере деятельности организации.

Специалисты по корпоративной защите от угроз информационной безопасности нужны во всех отраслях экономики, в организациях различной формы собственности.

Нормативные правовые акты

Поскольку Описание компетенции содержит лишь информацию, относящуюся к соответствующей компетенции, его необходимо использовать на основании следующих документов:

- ФГОС СПО.
  - 10.02.03, «Информационная безопасность автоматизированных систем», Приказ Министерства образования и науки РФ от 28 июля 2014 г. № 806
  - 10.02.04, «Обеспечение ИБ телекоммуникационных систем», Приказ Министерства образования и науки РФ от 9 декабря 2016 г. № 1551
  - 10.02.05, «Обеспечение ИБ автоматизированных систем», Приказ Министерства образования и науки РФ от 9 декабря 2016 г. № 1553
- Профессиональный стандарт
  - 06.032 Специалист по безопасности компьютерных систем и сетей, приказ Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 года N 598н
  - 06.030 Специалист по защите информации в телекоммуникационных системах и сетях, приказ Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 года N 608н
  - 06.033 Специалист по защите информации в автоматизированных системах, приказ Министерства труда и социальной защиты РФ от 14 сентября 2022 г. № 525н
  - 06.053 Специалист по информационной безопасности в кредитно-финансовой сфере, приказом Министерства труда и социальной защиты
  - Российской Федерации от 28.11.2022 № 739н

Указать название ПС, год утверждения, номер, организацию, которая утвердила ПС

- ЕТКС. Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации (Утв. Приказом Минздравсоцразвития России от 22.04.2009 N 205
  - Техник по технической защите информации
  - Специалист по обеспечению безопасности информации в ключевых системах информационной инфраструктуры
  - Администратор по обеспечению безопасности информации

- Отраслевые/корпоративные стандарты

— ISO/IEC 27001. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности.

- Квалификационные характеристики (профессиограмма)

— ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»
— ГОСТы ГОСТ Р ИСО/МЭК 27002-2021. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности
— ГОСТ Р ИСО/МЭК 15408-3-2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий
— ГОСТ Р 57580.1 – 2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер»;
— ГОСТ Р 57580.2.-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия».

Перечень профессиональных задач специалиста по компетенции определяется профессиональной областью специалиста и базируется на требованиях современного рынка труда к данному специалисту.

№ п/п	Виды деятельности/трудовые функции
1	Организация работы и охрана труда
2	Обслуживание средств защиты информации в операционных системах
3	Исследование (аудит) организации с целью защиты от угроз информационной безопасности
4	Разработка и реализация политик безопасности в системах корпоративной защиты информации от внутренних угроз ИБ
5	Анализ и защита сетевого трафика
6	Установка и администрирование подсистем защиты информации в операционных системах
7	Анализ выявленных инцидентов и угроз безопасности