Профессиональная проба по компетенции «Сетевое и системное администрирование» знакомит учащихся с основными функциями и обязанностями администратора компьютерных сетей, дает представление об области профессиональной деятельности сотрудников ИТ отделов и служб организаций, знакомит с основными понятиями и специальными терминами.

В наши дни одним из наиболее актуальных вопросов защиты корпоративной информации – обеспечение безопасности от внутренних утечек по техническим каналам связи. Одна из главных угроз корпоративной информационной безопасности – неправомерные действия 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.).

Необходимость защиты от внутренних угроз информационной безопасности не только доказана на практике, но и упомянута в ключевых международных стандартах по организации и менеджменту информационной безопасности (например, в ISO/IEC 27001).

Технологии корпоративной защиты от внутренних угроз информационной безопасности, относящиеся к классу data Leak Prevention (DLP) позволяют выявлять и предотвращать утечки конфиденциальной информации и персональных данных, защищать компании от мошенничества, воровства и коррупции, детектировать неправомерные действия сотрудников и нецелевое использование корпоративных ресурсов. Системы корпоративной безопасности позволяют однозначно выявлять инциденты и дают весь необходимый набор инструментов для проведения внутренних расследований и дальнейшей правовой защиты корпоративных интересов.

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 DLPсистем, 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.