Работодатель: Авиакомпания АО «Uzbekistan Airways».

Подразделение: Отдел администрирования и кибербезопасности Управление IT инфраструктуры, цифровизации и кибербезопасности.

Ставка: 1,00.

Зарплата: согласно штатному расписанию.

Требуемый опыт работы: не менее 3-х лет.

Форма занятости: полная занятость.

Режим работы: полный рабочий день.

Требования:

- Гражданство: Республика Узбекистан;
- Высшее оконченное образование по информационно-коммуникационным технологиям.
- Владеть узбекским, русским и английским языками в объёме, необходимом для выполнения своих должностных обязанностей.
- Стаж работы в аналогичной должности – не менее 3-х лет.
- Фундаментальные знания по кибербезопасности и администрированию.
- Сертификаты (дипломы и т.п.) подтверждающие дополнительные знания, навыки и квалификации по IT-технологиям – приветствуется.
- Сертификат о владении английским языком: приветствуется.

Обязанности:

- Выполнение установленных должностной инструкцией требований, а также:
- Соблюдать требования конфиденциальности.
- Обеспечивать бесперебойное функционирование локальных и корпоративной сетей, программно-аппаратного комплекса IT инфраструктуры, корпоративных сервисов и ресурсов АО.
- Обеспечивать администрирование программно-аппаратного комплекса IT инфраструктуры, корпоративных сервисов и ресурсов АО, в рамках компетенции отдела.

- Обеспечивать установку обновлений программного обеспечения на программно-аппаратных комплексах IT инфраструктуры АО, относящихся к компетенции отдела.
- Проводить необходимые мероприятия по обеспечению комплексной защиты «конечных точек».
- Обеспечивать информационную безопасность IT инфраструктуры АО.
- Выявлять, анализировать, и принимать участие в устранении инцидентов информационной безопасности и уязвимости информационных систем и других компонентов IT инфраструктуры АО.
- Определять возможные угрозы безопасности информации, осуществлять поиск уязвимостей программного и аппаратного обеспечения.
- Постоянно проводить работу по выявлению возможных каналов утечки конфиденциальной информации при эксплуатации информационно-коммуникационных систем АО и несанкционированного вмешательства в процесс их функционирования.
- Консультировать сотрудников АО по вопросам обеспечения информационной безопасности и защиты информации.
- Проводить практические мероприятия по предотвращению незаконного вмешательства в процесс функционирования системы и несанкционированного доступа к информации.
- Составлять информационные обзоры по обеспечению информационной безопасности и технической защите информации.
- Своевременно и качественно выполнять работы, в соответствии с годовыми и квартальными планами.
- Готовить и исполнять планы мероприятий, направленные на защиту IT инфраструктуры АО от различных угроз информационной безопасности.
- Проводить исследования с целью определения наиболее целесообразных практических решений в пределах поставленной задач.
- Изучать и обобщать опыт работы иных организаций по использованию способов обеспечения информационной безопасности, защиты информации и технических средств.
- Выполнять оперативные задания.
- Принимать участие в разработке и регулярной актуализации единой политики (концепции) обеспечения информационной безопасности АО, включая определение требований к системе защиты информации АО.
- Принимать участие в подготовке годовых и квартальных планов работы отдела.

- Разрабатывать и согласовывать технические задания на создание (модернизацию) объектов IT инфраструктуры АО, в части касающейся.
- Участвовать в расследовании причин возникновения аварийных ситуаций.
- Реализовывать принятые руководством АО решения по обеспечению информационной безопасности, защите информации.
- Осуществлять внедрение систем управления информационной безопасностью, защиты информации.
- Анализировать и оценивать эффективность предусмотренных мер по защите информации, в том числе конфиденциальной информации и персональных данных в АО.
- Готовить предложения по приобретению необходимого оборудования и программного обеспечения к нему.
- Принимать участие в подготовке технических требований по приобретению отдельных видов товаров, работ и услуг, закупаемых АО, в пределах компетенции отдела.
- Готовить предложения по приведению эксплуатируемых автоматизированных систем АО в соответствие происходящим изменениям действующего законодательства Республики Узбекистан в части обеспечения информационной безопасности.
- И другие.

Условия:

- Официальное трудоустройство;
- 5-дневная рабочая неделя, с 09:00 ч до 18:00 ч;
- Своевременная стабильная заработная плата;
- Испытательный срок: 3 месяца.

Ключевые навыки:

- Узбекский язык – B2 – средне-продвинутый уровень
- Русский – B2 – средне-продвинутый уровень
- Английский – B2 – средне-продвинутый уровень
- Знание TCP/IP
- Понимание модели OSI
- Умение распознать следствие/причины некорректной работы ПО или техники
- Анализ сетевого трафика

- Анализ защищенности сетевой инфраструктуры
- Знание почтовых и файловые служб основных ОС
- Умение выполнять анализ информационной защищенности
- Выявления угроз ИБ на основе сведений об уязвимостях (классификация угроз, формирование рекомендаций по устранению уязвимостей и минимизации бизнес-рисков)
- Управление рисками;
- Построение защищенной инфраструктуры

Резюме для рассмотрения отправлять по следующему электронному адресу:

Alexey.Kirillov@uzairways.com

Erkin.Alimov@uzairways.com