



## **Администратор информационной безопасности**

### **Должностные обязанности:**

- Анализ внешних угроз, уязвимостей, в том числе уязвимостей корпоративных систем, и разработка мер по их предотвращению;
- Мониторинг доступа работников Банка к информационно-вычислительным ресурсам попыток несанкционированного доступа, состояния систем защиты информации и объектов информатизации, в том числе с использованием инструментальных средств;
- Мониторинг и анализ трафика системы электронной почты и сети Интернет;
- Мониторинг системы обеспечения информационной безопасности и контроль защитных мер;
- Анализ Log-файлов серверов и активного сетевого оборудования Банка;
- Осуществление проверок соблюдения требований информационной безопасности;
- Участие в расследованиях инцидентов информационной безопасности;
- Участие в проверках по соблюдению требований информационной безопасности в структурных подразделениях Банка;
- Участие в процессе обучения и проведении инструктажа сотрудников Банка по вопросам обеспечения информационной безопасности.

### **Требования к кандидатам:**

- Образование – высшее в области ИБ/ИТ;
- Опыт работы в области информационной безопасности от 2 лет;
- Знание азербайджанского языка;
- Знание английского и русского языка (в объеме, достаточном для чтения технической документации по линиям информационных технологий и информационной безопасности);
- Ответственность, организованность, пунктуальность, аккуратность, хорошие коммуникативные качества;
- Умение работать самостоятельно;
- Энтузиазм в повышении собственной квалификации и приобретении новых навыков;
- Знание принципов работы компьютерных сетей, протоколов TCP/IP, межсетевых экранов, IPS, SIEM, DLP ;
- Знание и понимание принципов работы, функциональных возможностей и ограничений ОС MS Windows (желателен опыт работы с ОС \*nix);
- Экспертные знания современных угроз, уязвимостей и технологий защиты;
- Опыт использования сетевых сканеров уязвимости (Qualys, Nessus, Max Patrol) и анализа защищенности;
- Знание основ обеспечения безопасности web-приложений. Опыт конфигурации Web Application Firewall;
- Хорошее знание типовых инцидентов безопасности и умение определять их параметры для реализации в SIEM. Опыт работы с SIEM приветствуется

- Знание платформы виртуализации VMware и обеспечения ее безопасности;
- Знание сетевого оборудования Cisco, Palo Alto, F5 BIG-IP приветствуется;
- Наличие сертификатов в области информационной безопасности будет в пользу при выборе кандидата.

Заинтересованные лица могут отправить форму автобиографии (CV) на электронный адрес: [cv@accessbank.az](mailto:cv@accessbank.az) Просьба указать название вакансии в теме письма!