**РУКОВОДИТЕЛЬ СЛУЖБЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**Квалификационные требования:**

- минимум степень бакалавра в области информационных технологиях или смежных областях

- свободный украинский, продвинутый английский

- опыт работы от 5 лет в области IT-безопасности. Желательно в банковской сфере.

- желательно наличие профессиональных сертификаций. Например, CISSP, CISA, CISM и др.

- опыт управления командой

- опыт управления изменениями и бизнес-процессами является идеальным в сочетании с проверенной практикой реализации крупномасштабных программ изменений

**Ожидания:**

Лидерские навыки - способные расширить возможности и возглавить ИТ-команду для достижения бизнес-целей и целей ИТ-безопасности.

Навыки управления персоналом - обеспечение руководства, мониторинг производительности, мотивация персонала и создание позитивной рабочей среды.

Способность адаптироваться к быстро меняющемуся IT-ландшафту и идти в ногу с новейшим мышлением и новыми технологиями в области безопасности.

Стремится к переменам, демонстрируя впечатляющую способность продвигать стратегию ИТ-безопасности вперед.

Аналитический склад ума, способность управлять многочисленными источниками информации и предоставлять старшему руководству отчеты по анализу данных.

Сильная клиентоориентированность - в состоянии удовлетворить требования внутренних и внешних клиентов.

Отличные коммуникативные навыки - обеспечение устной и письменной коммуникации, которая является незаменимой как для непосредственных подчиненных, так и для старшего руководства, а также для других заинтересованных сторон.

Гибкий и адаптируемый - способный менять направление в случае необходимости и демонстрирующий гибкость для удовлетворения новых требований.

Формирует деловое партнерство, способствующее продвижению стратегии ИТ-безопасности.

Может принимать решения, которые хорошо информированы и своевременны.

Творческое мышление - умение смотреть на альтернативы и рассматривать новые способы мышления для решения проблем.

Многозадачность - может управлять несколькими одновременно выполняемыми проектами и устанавливать приоритеты требований.

**Задачи:**

- Разработка и реализация стратегии внедрения технологий информационной безопасности

- Проведение оценки рисков для ИТ-безопасности и составление отчетов о путях минимизации угроз.

- Мониторинг уязвимостей безопасности и угроз взлома в сетевых и хост-системах.

- Отслеживание последних инноваций в области IT-безопасности и отслеживание новейших технологий в сфере кибербезопасности.

- Обеспечение непрерывности бизнеса

- Общение с ключевыми заинтересованными сторонами об угрозах ИТ-безопасности

- Внедрение эффективного процесса информирования об инцидентах в области безопасности

- Наблюдение за расследованием сообщений о нарушениях безопасности

- Разработка стратегий по борьбе с инцидентами в области безопасности и инициированию расследований

- Управление командой IT-безопасности, экспертами и консультантами по безопасности

- Соблюдение новейших правил и требований по соответствию

- Управление повседневной деятельностью и реализация стратегии IT-безопасности

- Проведение непрерывной оценки текущей практики и систем IT-безопасности и выявление областей, нуждающихся в улучшении

- Проведение аудитов безопасности и оценок рисков

- Внедрение новых технологических подходов в области безопасности и внедрение решений нового поколения.

- Наблюдение за управлением отделом IT-безопасности, обеспечение руководства командой и развитие персонала

- Ведение проектов изменений и создание новых IT-возможностей.

- Разработка стратегий и внедрение ИТ-решений для минимизации риска кибератак.

- Обзор, анализ и предоставление информации

- Управление бюджетом ИТ-безопасности и доведение его до сведения соответствующих сторон.

- Отчитывается перед советом директоров и является активным членом группы высшего руководства.