В АО «РН-Няганьнефтегаз» осуществляется подбор кандидатов на должность

**Главный специалист по информационной безопасности АСУТП**

Работа в отделе информационных технологий, телекоммуникаций и информационной безопасности

*Основные функции:*

1.      Выполняет мероприятия по обеспечению информационной безопасности в ключевых автоматизированных системах управления технологическими процессами Общества.

2.      Осуществляет создание встроенных средств защиты информации для автоматизированных систем управления технологическими процессами и контрольно-измерительных приборов (далее – АСУТП) Общества.

3.      Производит оценку защищенности и анализ уязвимостей встроенного программного обеспечения (далее – ПО) (контроллеры АСУТП, релейная защита автоматики (далее – РЗА), устройства связи) и системного ПО (SCADA, комплексы ПО систем учета электроэнергии).

4.      Осуществляет оценку соответствия отраслевым требованиям встроенных средств защиты встроенного и системного ПО автоматических систем технологического управления.

5.      Организовывает и проводит испытание оборудования Общества на соответствие требованиям информационной безопасности федеральной службы по техническому и экспертному контролю (далее – ФСТЭК) России.

6.      Разрабатывает программы/методики испытаний и тестирование программных и аппаратных компонентов АСУТП на совместимость со средствами защиты информации. Составляет отчеты о соответствии предъявляемым требованиям.

7.      Осуществляет подготовку технической документации по проектам внедрения средств защиты (технические задания, рабочие инструкции, технические паспорта, схемы).

8.      Осуществляет координацию работ по управлению рисками информационной безопасности (далее – ИБ) АСУТП Общества.

9.      Организует разработку и документирование (в виде локальных нормативных документов) требований, направленных на снижение выявленных рисков ИБ в АСУТП.

10.  Обеспечивает рассмотрение и согласование требований, технических решений и средств в процессе разработки, проектирования, внедрения и модернизации АСУТП Общества.

11.  Организует подготовку предложений по обеспечению ИБ АСУТП, а так же согласование требований с руководителями структурных подразделений Общества, участвующих в процессах разработки, внедрения, сопровождения и эксплуатации АСУТП.

12.  Обеспечивает контроль полноты и качества реализации процессов и мер по обеспечению ИБ АСУТП..

*Образование:*

* Высшее профессиональное образование по специальности «Автоматизация технологических процессов и производств», «Защищенные автоматизированные системы управления», «Обеспечение информационной безопасности распределенных информационных систем», «Анализ безопасности информационных систем», «Создание автоматизированных систем в защищенном исполнении».

Приветствуется наличие сертификатов в области технической защиты информации в автоматизированных системах управления производственными и технологическими процессами, информационной безопасности, аудита или управления ИТ, управления проектами.

*Стаж работы:*

* По специальности в должности ведущего специалиста по информационной безопасности АСУТП не менее 3 лет.

*Знания и навыки:*

* Нормативные акты, регламентирующие сферу информационной безопасности (руководящие документы ФСТЭК, ФСБ, Роскомнадзора, Постановления Правительства, ФЗ и др.);
* Методология опыт проведения оценки и анализа рисков ИБ (CRAMM, RiskWatch, Cobra и др.);
* Методики и стандарты в области ИБ и аудита ИБ (Cobit, ITIL, ISO 27001, ISO 17799, NIST SP 800), опыт проведения внутреннего/внешнего аудита ИБ АСУТП;
* Основы технологий обеспечения информационной безопасности (VPN, AAA, PKI, IDS/IPS/IDP);
* Опыт работы по внедрению и сопровождению проектов и систем ИБ (антивирусы, защита серверов, рабочих станций, локальных вычислительных сетей АСУТП);
* Навыки работы со средствами защиты информации, встроенными средствами защиты ОС и активного сетевого оборудования, программирования и работы с БД (не обязательно очень глубокие);
* Опыт оценки защищенности систем, разработки модели угроз, выработки мер защиты;
* Опыт разработки технической и аналитической документации;
* Опыт расследования инцидентов безопасности, сбор доказательной базы, форензика.
* Знание английского языка (технический) на уровне чтения и понимания.

*Компьютерная грамотность:*

* Опытный пользователь стандартного пакета Microsoft Office;
* Специализированное ПО:

- система электронного документооборота (DIRECRUM);

- интегрированная информационная система управления финансово-хозяйственной деятельностью SAP/R3;

- автоматизированные средства управления проектами (MS Project и/или другие);

- Kaspersky;

- CheckPoint;

- VipNet.

- опыт работы с Windows, Linux, QNX (желательно) и другими ОСРВ;

- знание профильного ПО (MaxPatrol, Cisco ASA и т.д.);

- экспертные знания в узкоспециализированных системах (например SCADA/ERP/SS7/Hardware);

- знание операционных систем и встроенных механизмов защиты информации MS Windows, UNIX (Linux, Solaris, BSD, HP-UX);

- знание принципов построения и функционирования сетей и протоколов стека TCP/IP.

*Требования к личным качествам:*

* Ответственность, стрессоустойчивость, коммуникабельность.

Кандидатам направлять резюме с пометкой **Главный специалист по ИБ АСУТП** и собственноручным согласием на обработку своих персональных данных на электронный адрес nyg-resume@nng.rosneft.ru