В целях повышения уровня защищённости информационных систем, обеспечения устойчивости к внутренним и внешним угрозам, а также соблюдения требований законодательства Республики Беларусь в области информационной безопасности, в организации необходимо ввести должность специалиста по информационной безопасности.

Функционал:

Специалист будет отвечать за разработку, внедрение и контроль выполнения мер, направленных на защиту информации от несанкционированного доступа, утраты, изменения и распространения. Особое внимание будет уделено мониторингу и реагированию на инциденты с использованием SIEM-систем, а также предотвращению утечек данных с помощью DLP-решений.

Введение должности соответствует положениям Закона Республики Беларусь «Об информации, информатизации и защите информации», а также требованиям технических нормативных правовых актов (ТНПА), включая СТБ ISO/IEC 27001 и СТБ ISO/IEC 27002. Учитываются также новые положения законодательства, предусматривающие административную ответственность и штрафы за киберинциденты (ст. 23.11 КоАП, до 600 базовых величин), включая утечку персональных данных и нарушение режима защиты информации.

Специалист будет участвовать в анализе рисков, расследовании инцидентов, разработке и реализации корректирующих и предупреждающих мер. В рамках технической инфраструктуры будет обеспечено внедрение и настройка SIEM-систем для централизованного мониторинга событий безопасности, а также DLP-систем для контроля каналов передачи конфиденциальной информации.

Основные функции специалиста:

* разработка и актуализация политики информационной безопасности включая положения о мониторинге, реагировании на инциденты, управлении доступом и защите персональных данных;
* проведение оценки рисков и уязвимостей информационных систем с использованием методик, соответствующих требованиям ISO/IEC 27005 и национальных стандартов;
* внедрение криптографических, организационных и технических мер, включая настройку и сопровождение SIEM и DLP-систем;
* контроль соблюдения требований информационной безопасности сотрудниками включая проведение проверок, аудита поведения пользователей, анализ инцидентов и нарушений;
* участие в расследовании инцидентов, связанных с нарушением безопасности с документированием событий, взаимодействием с правоохранительными органами и подготовкой отчётности для регуляторов (КГБ, ОАЦ и др.);
* взаимодействие с внешними аудиторами и регуляторами, а также подготовка к проверкам, предоставление необходимой документации, сопровождение аудитов;
* обучение и консультирование сотрудников, включая проведение инструктажей, семинаров и консультаций по вопросам защиты информации, включая правила работы с конфиденциальными данными и предотвращение инцидентов.