У нас есть 3 направления, которые требуют несколько разных подходов.

* Инфраструктура (домен, политики, сеть, сервера БД как таковые, сервера приложений)
  + Опыт администрирования (проектирование систем прав, настройка автоматизации аудита, выбор СЗИ)
  + Рекомендации вендоров
  + Общие стандарты, методики и концепции
* Внешние системы (сайт, интеграция с ФК, СМС, почта)
  + Общие способы обхода и проникновения, Соц.
  + Архитектура и особенности защиты веб-приложений
  + Периметр и его охрана
* Внутренние системы
  + Архитектура систем аутентификации, ролевые модели
  + Взаимодействие с инфраструктурой анализ кода приложений

## Обязанности:

* Анализ структуры бизнес-процессов и информационных систем с точки зрения информационной безопасности;
* Аудит информационной безопасности;
* Расследование инцидентов информационной безопасности
* Подготовка предложений по созданию/развитию систем обеспечения ИБ;
* Разработка ТЗ на изменение информационных систем для обеспечения информационной безопасности;
* Проектирование комплексных систем обеспечения ИБ, выбор СЗИ;
* Взаимодействие с техническими и другими внутренними подразделениями для реализации мер защиты и обеспечения ИБ
* Разработки политик, стандартов и регламентов по информационной безопасности
* Участие в мероприятиях по повышению осведомленности сотрудников в вопросах ИБ, консультация сотрудников по вопросам обеспечения ИБ
* Оценка качества и эффективности применяемых мер защиты информации
  + Построение безопасной архитектуры веб приложений, проведение внутренних пентестов, анализ защищенности веб-приложений, анализ кода.
  + Поиск и анализ уязвимостей в внутреннем ПО;
  + Разработка алгоритмов поиска уязвимостей;

## Требования:

### Образование и опыт

* Высшее образование в области информационных технологий (предпочтительно по направлению «информационная безопасность»)
* Опыт работы не менее 2-х лет в области информационной безопасности либо администрирования/разработки ИТ решений в части ИБ.
* Опыт разработки внутренних документов по ИБ;

### Технологии и инструменты

* Знания службы Active Directory, ОС семейства MS Windows, MS Windows Server на уровне администратора.
* Знание архитектуры современных информационных систем (инфраструктура, виртуализация, СУБД, бизнес-приложения);
* Понимание работы сетей на базе TCP/IP, основных сетевых протоколов, веб-протоколов
* Опыт работы с популярными СУБД (особенно MS SQL Server);
* Знание продуктов и технологий обеспечения безопасности прикладного слоя/бизнес-приложений (таких как: построение моделей угроз и нарушителя; защита от НСД: аутентификация, антивирусная защита, межсетевое экранирование, обнаружение вторжений, анализ защищенности, защита от утечек, криптографическая защита информации, защита виртуализации; защита каналов связи);
* Опыт работы со сканерами веб-уязвимостей: (напр. Acunetix, OWASP Zed Attack Proxy, w3af, Skipfish, Websecurify, и т.д);

### Стандарты и методики

* Знание текущих трендов по обеспечению информационной безопасности, программных средств защиты;
* Знания стандартов и лучших практик в области ИБ и ИТ: 152-ФЗ, 149-ФЗ, приказы ФСТЭК 17, 21, 31, ISO27XXX, ITIL/ITSM и т.п.;
* Навыки практической компрометации и защиты веб приложений, знание основных типов атак и уязвимостей;
* Понимание природы уязвимостей ПО, методов взлома;

### Личные качества

* Ориентированность на бизнес-результат
* Аналитический склад ума
* Умение работать в команде

## Является преимуществом:

* Наличие:
  + статуса «Certified Information Systems Auditor» (CISA), «Certified Information Security Manager» (CISM) и/или «Certified Information Systems Security Professional» (CISSP).
  + Сертификации в области ИБ;
  + Дополнительное образование в области ИБ, курсы по сетевым технологиям, технологиям защиты информации (Код Безопасности, Инфотекс, Imperva, Arbor, Cisco, McAfee (StoneSoft), DallasLock, TrendMicro, MaxPatrol, Касперский, InfoWatch, CyberArc и др.вендорам), курсы по вопросам аттестации АС, курсы по вопросам криптографии;
  + публикаций на тематических форумах и в блогах;
  + опубликованных данных об уязвимостях, обнаруженных вами;
* Опыт участия в CTF или bug-bounty программах;
* Опыт работы с DLP -средствами защиты информации
* Опыт проведения Аудита ИБ на соответствие ISO 27001
* Знание ОС семейства Linux в части ИБ.
* Навыки программирования на одном следующих языков: Java, C#, С++, T-SQL;