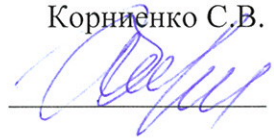
Утверждаю:
Директор по информационным технологиям -
начальник департамента ИТ
ОАО «МРСК Центра»
Дудин А.В.

Техническое задание

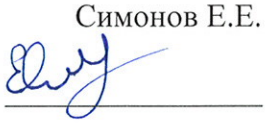
на «Консультационные услуги по подготовке Отчета о состоянии информационной безопасности АСТУ»

Шифр: «ИБ АСТУ»

Согласовано
Заместитель начальника
Департамента ИТ
Корниенко С.В.



Согласовано:
Начальник управления ИТ
ОАО «МРСК Центра»
Симонов Е.Е.



2012г.

Содержание

1. Общие положения

1.1. Настоящее техническое задание определяет состав, порядок и объем работ по анализу информационной безопасности автоматизированной системы технологического управления (АСТУ) ОАО «МРСК Центра».

1.2. Наименование работы: Консультационные услуги по подготовке Отчета о состоянии информационной безопасности АСТУ (далее – анализ ИБ АСТУ).

1.3. Шифр работы: «ИБ АСТУ».

1.4. Заказчик работы: ОАО «МРСК Центра» (далее – Общество).

1.5. Исполнитель работы: определяется по итогам конкурсной процедуры.

1.6. Финансирование работ ведется за счет средств Заказчика. Порядок финансирования работ определяется договором между Заказчиком и Исполнителем.

1.7. Плановые сроки окончания работы – не позднее 1 октября 2012 года.

2. Цель и задачи проведения анализа ИБ АСТУ

2.1. Основные цели проведения работы - получить независимую оценку степени защищенности прикладной, системной и сетевой инфраструктуры АСТУ, а также их соответствие действующим в компании политикам и процедурам по информационной безопасности.

2.2. В ходе достижения поставленной цели планируется решить следующие задачи:

- выбор и согласование с заказчиком модели угроз;
- определение вероятного нарушителя информационной безопасности;
- выбор и согласование с заказчиком методики проведения обследования;
- проведение анализа защищенности прикладной, системной и сетевой инфраструктуры АСТУ;
- проведение теста на проникновение в АСТУ;
- оценка используемых средств обеспечения информационной безопасности (относительно выбранной модели вероятного нарушителя).

3. Требования к содержанию работ по анализу ИБ АСТУ

3.1. Определение границ анализа ИБ АСТУ должно учитывать распределение и структуру основных информационных потоков АСТУ, в которых содержится критичная информация.

3.2. Сбор, анализ и обобщение исходных данных АСТУ должны охватывать всю необходимую для проведения анализа ИБ информацию, касающуюся информационной инфраструктуры АСТУ, методов и механизмов обеспечения защиты информации, а также нормативных и организационно-распорядительных документов

3.3. При сборе данных должны использоваться следующие основные источники информации:

- интервью со специалистами Заказчика с целью выяснения особенностей информационной инфраструктуры АСТУ, размещения информационных ресурсов, их ценности и критичности для работы организации, состава нормативных и регламентирующих документов, проектной документации и организационной структуры;
- обследование объектов АСТУ с целью проведения инвентаризации информационных ресурсов, выяснения условий эксплуатации, подключений и соединений оборудования, устройств и каналов связи;
- средства мониторинга загрузки оборудования, линий и каналов передачи с распределением по времени, направлениям передачи, протоколам и т.п.;
- рекомендации производителей оборудования и программного обеспечения по использованию продуктов и общим вопросам создания информационных систем;
- организационно-распорядительная документация (Политики ИБ, инструкции, регламенты и руководства пользователей и администраторов), регламентирующая работу АСТУ;
- используемые программно-технические средства и методы защиты информации, настройки данных средств, режимы функционирования и эксплуатации.

3.4. Для выявления уязвимостей информационной инфраструктуры АСТУ должна использоваться комбинация автоматизированного и ручного поиска.

3.5. При автоматизированном поиске уязвимостей АСТУ должны использоваться современные, хорошо себя зарекомендовавшие инструментальные средства.

3.6. Ручной поиск уязвимостей должен применяться в случае, когда автоматизированный поиск признается Исполнителем

неэффективным, а также в процессе выявления уязвимостей в применяемых организационных мерах защиты информации.

3.7. При выявлении уязвимостей АСТУ должен быть сформирован перечень уязвимостей технических (программных и программно-аппаратных) средств, в том числе:

- ошибки при проектировании и внедрении;
- ошибки при настройке и конфигурации;
- уязвимости в реализации программного обеспечения (отсутствие протоколирования, ошибки в скриптах и исполняемых модулях, переполнение буфера, перехват (раскрытие) паролей);
- возможность осуществления атак «отказ в обслуживании»;
- недостатки механизмов управления учетными записями и парольной информацией;
- уязвимости программного обеспечения Интернет–сервисов;
- уязвимости баз данных.

3.8. В рамках работ по выявлению уязвимостей АСТУ должен проводиться анализ технологической защищенности, на предмет:

- совместимости используемых средств защиты информации;
- уязвимости используемых протоколов;
- анализа защищенности архивных копий и процедур резервного копирования.

3.9. Процесс выявления уязвимостей должен охватывать действующие процессы по управлению информационной безопасности АСТУ, а также нормативные и организационно-распорядительные документы, а именно:

- изучение и оценку процессов системы управления информационной безопасности, включая, но, не ограничиваясь, процессами разработки и ввода в действие политик безопасности, управления событиями и инцидентами, ознакомления и обучения пользователей и т.п.;
- анализ политики информационной безопасности;
- анализ инструкций, регламентирующих использование средств и методов защиты информации (инструкции по организации парольной защиты, антивирусной защиты, резервного копирования, доступа к критичной информации и ресурсам сети Интернет, и др.);
- анализ организационной структуры обслуживающего персонала и должностных инструкций.

4. Требования к документированию

4.1. В состав отчетной документации должны включаться следующие документы:

- Согласованное с Заказчиком описание границ анализа ИБ АСТУ;
- Перечень критичных информационных ресурсов АСТУ;
- Перечень объектов АСТУ, содержащих уязвимости;
- Результаты анализа эффективности мер и средств защиты информации, применяемых в АСТУ;

4.2. Вся документация должна быть изложена на русском языке, подготовлена как в напечатанном виде, так и на магнитном носителе в формате MS Word для Windows.

4.3. На основании сведений, полученных в процессе проведения обследования ИБ АСТУ, должен быть подготовлен итоговый отчет, содержащий информацию о результатах.

4.4. Отчет о состоянии ИБ АСТУ должен содержать в себе следующие сведения:

- описание границ анализа ИБ АСТУ;
- структурированную информацию об инфраструктуре и прикладных информационных системах АСТУ, а также об используемых в них мерах и средствах защиты информации;
- перечень идентифицированных информационных ресурсов АСТУ, ранжированных по степени критичности;
- оценки эффективности применяемых мер и средств защиты информации;

4.5. Отчет о состоянии ИБ АСТУ должен предоставить информацию для возможного последующего технического проектирования или модернизации системы обеспечения информационной безопасности.

5. Требования к подрядной организации

5.1. Участник конкурса должен обладать гражданской правоспособностью в полном объеме для заключения и исполнения Договора, должен быть зарегистрирован в установленном порядке и иметь соответствующие свидетельства на допуски к данным видам работ.

5.2. Участник конкурса не должен являться неплатежеспособным или банкротом, находится в процессе ликвидации или экономическая деятельность участника конкурса должна быть приостановлена. На имущество участника конкурса не должен быть наложен арест.

5.3. Участник конкурса должен обладать необходимыми профессиональными знаниями и опытом, управленческой

компетентностью, репутацией, иметь ресурсные возможности (финансовые, материально-технические, производственные, трудовые).

5.4. Участник конкурс должен иметь следующие лицензии:

- лицензия ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации;
- лицензию ФСТЭК России на деятельность по разработке и (или) производству средств защиты конфиденциальной информации.

5.5. Предметом конкурентного отбора является соответствие участника конкурса общим требованиям, предъявляемым к подрядной организации, а так же:

- стоимость и сроки оказания услуг, предложенных участником конкурса;
- опыт деятельности по оказанию аналогичных услуг не менее 2 лет;
- способность обеспечить соответствие оказываемых услуг нормативно-методологическим требованиям, предъявляемым регуляторами в области информационной безопасности Российской Федерации, распорядительным документам ОАО «Холдинг МРСК», ОАО «МРСК Центра» (опыт работы с предприятиями электроэнергетики);
- наличие действующей системы менеджмента качества, подтвержденное сертификатом соответствия стандарту ГОСТ Р ИСО 9001-2008.