**Техническая спецификация**

**Проведение аудита внешнего периметра сети Биржи   
(Анализ защищенности корпоративной сети)**

В целях оказания услуг необходимо провести тестирование на проникновение в информационную инфраструктуру АО "Казахстанская фондовая Биржа" (далее Заказчик), попытки эксплуатации уязвимостей системного и прикладного программного обеспечения, нагрузочные тесты включающие имитацию атак "отказ в обслуживании", и тесты по социальной инженерии.

Цель проведения работ по тестированию на проникновение в информационную инфраструктуру Заказчика является оценка состояния устойчивости информационных ресурсов Заказчика к атакам со стороны сети Интернет, а также проверка работников организации Заказчика на умение распознать и корректно среагировать на атаки, проводимые методами социальной инженерии.

**Объекты обследования:**

1. В рамках проведения работ по тестированию на проникновение необходимо обследовать следующие информационные ресурсы Заказчика:

* www.kase.kz
* is2in.kase.kz
* sftp.kase.kz
* [ftp.kase.kz](ftp://ftp.kase.kz)
* clearing.kase.kz

1. Провести автоматизированный поиск уязвимостей во внешнем периметре корпоративной сети Заказчика.
2. Провести атаку методом социальной инженерии для чего подготовить и распространить фишинговое письмо на почтовые адреса работников Заказчика.

**Первоначальная информация.**

Для проведения тестирования Заказчик может предоставить Исполнителю следующую первоначальную информацию:

1. Сетевые адреса и сетевые порты, по которым доступны обследуемые ресурсы.
2. Учетные записи непривилегированных пользователей, если ИС предполагает работу с внешними клиентами, а процесс регистрации не является открытым.
3. Перечень сетевых адресов (для проведения автоматизированного поиска уязвимостей во внешнем периметре заказчика следующие данные).
4. Перечень e-mail адресов работников Заказчика (для проведения атак методом социальной инженерии).

**Модель злоумышленника.**

В качестве потенциального нарушителя рассматривается лицо или группа лиц, которые в результате умышленных действий, со злым умыслом или без такового могут реализовать различные угрозы информационной безопасности. При этом нарушитель не является авторизованным и/или привилегированным пользователем обследуемых информационных систем, имеет первоначальную информацию об информационных ресурсах в рамках, описанных в разделе "Первоначальная информация", и обладает практическим опытом проведения различных атак на информационные системы

**Результаты.**

Результаты проведенного анализа защищенности представляются в виде отчета на русском языке, содержащего:

* экспертное заключение по текущему состоянию устойчивости к атакам обследованных информационных ресурсов;
* список выявленных возможных уязвимостей;
* описание проведенных или возможных для проведения атак на информационные ресурсы;
* рекомендации по устранению выявленных уязвимостей и повышению защищенности от атак;
* заключение об уровне осведомленности персонала Заказчика в вопросах информационной безопасности

**Требования к содержанию отчета:**

* каждое предположение об уязвимостях информационных ресурсов, должно сопровождаться ссылкой на источник, на основании которой сделано предположение;
* выводы об устойчивости информационных ресурсов к атакам не должны основываться только на результатах автоматизированных средств поиска уязвимостей, а должны быть подкреплены практическими проверками (только для ИС обозначенных в п.1 раздела "Объекты обследования");

**Для осуществления полноценной услуги потенциальному Исполнителю необходимо иметь:**

* практический опыт проведения не менее двух работ по анализу защищенности корпоративной сети организаций и (или) тестов на проникновение *(подтвержденных актами выполненных работ (оказанных услуг)*;
* сертификаты по прохождению работниками потенциального поставщика обучения в сфере расследования компьютерных инцидентов *(предоставить копию сертификата и документы, подтверждающие сотрудничество такого работника с потенциальным поставщиком (например, выписка из штатного расписания, копия трудового договора и т.д.))*;
* прохождение работниками потенциального поставщика обучения по международным стандартам информационной безопасности – ISO 27001 *(предоставить копию сертификата и документы, подтверждающие сотрудничество такого работника с потенциальным поставщиком (например, выписка из штатного расписания, копия трудового договора и т.д.))*.

Срок оказания услуг – в течение 60 рабочих дней со дня подписания договора сторонами.