Извещение о проведении закупки
Фонд поддержки детей с тяжелыми жизнеугрожающими и хроническими заболеваниями, в том числе редкими (орфанными) заболеваниями, «Круг добра»

Номер извещения	17/2023
Наименование закупки	Оказание услуги по комплексному тестированию на проникновение в корпоративную информационную систему Фонда «Круг добра»
Способ проведения закупки	Закупка путем проведения переговоров о заключении договора (рассматривается заключение 1 договора)
Содержание и объем оказываемых услуг	Содержание оказываемых услуг и их объём определены в техническом задании (приложение №1 к Извещению).
Требования к участникам	Лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации. Лицензия ФСТЭК России должна распространяться на работы, предусмотренные пунктами «б» перечня видов работ и услуг, составляющих лицензируемую деятельность, указанного в Положении, утвержденном Постановлением Правительства Российской Федерации № 79 от 03.02.2012
Порядок расчетов	Оплата производится в течении 10 (десяти) рабочих дней с момента подписания Сторонами акта сдачи-приемки оказанных услуг.
Другие существенные условия	- По запросу представлять информацию и документы, относящиеся к предмету Договора, Министерству здравоохранения Российской Федерации и органам государственного финансового контроля в связи с заключенным между Министерством здравоохранения Российской Федерации и Фондом «Круг добра» Соглашением о предоставлении гранта в форме субсидии из федерального бюджета, для проверки соблюдения целей, условий и порядка предоставления Заказчику из федерального бюджета гранта в форме субсидии; - Указать в документах идентификатор соглашения о предоставлении из федерального бюджета Фонду «Круг добра» 0000000005622P6E0002, предоставляемых Заказчику (акт, счет на оплату, счет-фактура)

В случае заинтересованности в участии в переговорах на оказание услуги по комплексному тестированию на проникновение в корпоративную информационную систему Фонда «Круг Добра», просим направить до 14:00 (мск.врм) 2 октября 2023 года на электронный адрес office@kd-fund.ru информационное письмо с приложением следующих документов организации: коммерческие предложения с указанием стоимости и сроков выполнения работ, копии учредительных документов, свидетельства о государственной регистрации юридического лица, свидетельства о постановке на налоговый учет, документа об избрании руководителя, бухгалтерского баланса за прошедший год, справки об отсутствии задолженности перед бюджетом.

Приложение 1

Техническое задание на проведение анализа уровня защищенности

Информация о Заказчике		
Название компании*	ФОНД ПОДДЕРЖКИ ДЕТЕЙ С ТЯЖЕЛЫМИ ЖИЗНЕУГРОЖАЮЩИМИ И ХРОНИЧЕСКИМИ ЗАБОЛЕВАНИЯМИ, В ТОМ ЧИСЛЕ РЕДКИМИ (ОРФАННЫМИ) ЗАБОЛЕВАНИЯМИ, "КРУГ ДОБРА"	
Официальный сайт	https://xn--80abfdb8athfre5ah.xn--p1ai/	
Сфера деятельности	ФОНД ПОДДЕРЖКИ ДЕТЕЙ С ТЯЖЕЛЫМИ ЖИЗНЕУГРОЖАЮЩИМИ И ХРОНИЧЕСКИМИ ЗАБОЛЕВАНИЯМИ, В ТОМ ЧИСЛЕ РЕДКИМИ (ОРФАННЫМИ) ЗАБОЛЕВАНИЯМИ, "КРУГ ДОБРА"	
Контактное лицо*	Савкин Владимир	
Номер телефона*	моб: +7 916 571 5754; раб: +7 495 197 6264 (доб 281)	
Адрес электронной почты*	v.savkin@kd-fund.ru	
Информация о желаемых услугах		
Цель проведения работ	Оценка уровня защищенности инфраструктуры	*Пример:* *♦ Соответствие требованиям стандартов* *♦ Оценка уровня защищенности инфраструктуры* *♦ Проверка устойчивости к хакерским атакам* *♦ Иное*
Ожидаемые даты старта/финиша работ*	До 30.09.2023	*Пример: с 01.01.2019 по 31.03.2019 или до 31.03.2019*
Желаемый состав работ:* ♦ тестирование на проникновение ♦ анализ защищеннсти беспроводных сетей ♦ анализ защищенности веб приложений ♦ выявление нестойких паролей	тестирование на проникновение анализ защищенности беспроводных сетей анализ защищенности веб приложений выявление слабых паролей сканиерование уязвимостей	*Пример:* *Тестирование на проникновение и анализ защищенности веб приложений* *(Для каждой из работ, пожалуйста, заполните соответствующие страницы анкеты)*
Требуется ли проверка устранения выявленных уязвимостей*	Требуется проверка устранения выявленных уязвимостей	*Пример:* *♦ Требуется проверка устранения выявленных уязвимостей* *♦ Не требуется*
Дополнительные условия и пожелания		
Дополнительная информация, которую необходимо учесть при планировании работ и подготовке коммерческого предложения		*Укажите, пожалуйста, информацию, которая могла быть упущена или которую Вы считаете важной при планировании и проведении работ по тестированию на проникновение*

** - поля, обязательные для заполнения*

Внешний тест на проникновение		
Количество IP адресов*	внешний 90.154.49.82 лок. Сеть 192.168.0.1/23	*Укажите точное количество IP-адресов, входящих в область тестирования* *Пример: 20 или 172.20.10.0/24*
Количество проприетарных веб-приложений*	2	*Укажите количетво проприетарных ("готовых") веб-приложений, входящих в область внешнего теста. Указанные приложения НЕ должны относиться к услуге "Анализ веб-приложений". Примеры подобных приложений: Microsoft Outlook Web Access, Microsoft Skype For Business, аутентификационные веб-интерфейсы сервисов VPN (CheckPoint, Cisco SSLVPN), Atlassian Confluence, Jira, хранилище NextCloud и аналогичные* *Пример: 3*
Количество самописных веб-приложений*		*Укажите количетво самописных (разработанных самостоятельно или с привлечением заказчика) веб-приложений, входящих в область внешнего теста. Указанные приложения НЕ должны относиться к услуге "Анализ веб-приложений". Примеры подобных приложений: сервис контроля за рабочим временем сотрудников, сервис вакансий компании* *Пример: 3*
Есть ли временные ограничения	Нет ограничений	*Пример:* *♦ Есть, только в рабочее время с 09:00 до 18:00* *♦ Есть, только в рабочие дни* *♦ Нет ограничений*
Есть ли ограничения по интенсивности сетевого трафика		*Пример:* *♦ Есть, не более 20 Мб/с на узел*
Внутренний тест на проникновение		
Количество площадок проведения работ*	1	*Укажите количество площадок, на которых необходимо провести внутренний тест на проникновение* *Пример: 1*
Фактические адреса площадок проведения работ*	г. Москва, ул. Маросейка, д. 7/8, стр. 1, этажи 4 - 6	*Укажите адреса площадок* *Пример: 121096, г. Москва, ул. Василисы Кожиной, д. 1, корп. 1, этаж 8, комната 25*
Используемая модель нарушителя:* ♦ Легитимный пользователь (с предоставлением тестовой учетной записи) ♦ Гость (без предоставления учетной записи)	Легитимный пользователь и гость	*Укажите модель тестирования: с предоставлением тестовой учетной записи с привилегиями пользователя (легитимный пользователь) или без учетной записи (гость)* *Пример: гость*
Количество активных (живых) узлов сети*	192	*Укажите количество активных узлов сети (серверы, рабочие станции)* *Пример: 1000*
Количество доменов Active Directory*	1	*Пример: 1*
Тест на проникновение с применением методов социальной инженерии		
Количество сотрудников (адресов эл.почты), планируемых к участию в тестировании (фокус-группа)	90	*Укажите точное количество сотрудников, которых необходимо протестировать* *Пример: 100*
Формирование фокус-группы	Сбор адресов из открытых источников	*Адреса эл.почт может быть собран Исполнителем из открытых источников или предоставлен Вами. Укажите желаемый вариант* *Пример:* *♦ Сбор адресов из открытых источников* *♦ Передача адресов фокус-группы Заказчиком*
Дополнительное согласование фокус-группы	требуется	*Если формирование фокус-группы выполняется Исполнителем, укажите, требуется ли предварительно согласовать список эл.почт с Вами* *Пример: требуется*
Количество и типы сценариев:* ♦ Массовая рассылка - рассылка писем большому количеству сотрудников по одному разработанному сценарию ♦ Целевая рассылка - рассылка писем определенному сотруднику/группе сотрудников (например, подразделению) по индивидуально разработанному сценарию ♦ Целевая рассылка топ-менеджерам - рассылка писем топ-менеджерам по индивидуально разработанному сценарию	Массовая рассылка - 2 Целевая рассылка - 2	*Укажите тип и количество желаемых сценариев проведения теста.* *Пример: Массовая рассылка - 1, Целевая рассылка - 2*
Дополнительные условия и пожелания		
Дополнительная информация, которую необходимо учесть при планировании работ и подготовке коммерческого предложения	Всего в Фонде 10 отделов, соответсвенно могут быть минимум 10 различных сценариев целевой рассылки	*Укажите, пожалуйста, информацию, которая могла быть упущена или которую Вы считаете важной при планировании и проведении работ по тестированию на проникновение*

** - поля, обязательные для заполнения*

Информация о приложениях		
Количество веб приложений*	1	*Укажите точное количество приложений, входящих в область анализа* *Пример: 2*
Краткое описание особенностей каждого приложения (предназначение, функциональные особенности, и т.п.)*	Сайт Фонда kd-fund.ru, он же файловый обменник и CRM-система	*Кратко опишите каждое приложение* *Пример:* *Приложение1: интернет-магазин компьютерной техники* *Приложение 2: система ДБО для физических лиц*
URL-адреса каждого приложения (при возможности)	https://kd-fund.ru	*Пример:* *https://computer.store* *https://dbofiz.greenbank.ru*
Перечень использованных технологий при разработке приложений и введении их в эксплуатацию (языки программирования, фреймворки, CMS, ОС, СУБД и т.п.)	Embarcadero RAD Studio 11 Devart UniDAC FastReport VCL library Android SDK uniGUI Framework uniGUI HyperServer Elementor + Wordpress MS SQL Server + Transact-SQL	*Пример: Java, Spring Framevork, AngularJS, Linux, Apache, PostgreSQL*
В каком окружении планируется проведение анализа защищенности приложения: ♦ тестовая инфраструктура ♦ предпродуктивныая ♦ продуктивная	продуктивная	*Анализ может проводиться как на этапе тестирования, так и в продакшене. Укажите, в каком окружении будет проводиться анализ каждого приложения* *Пример: тестовая*
Планируются ли внесение изменений в приложения на протяжении работ по анализу защищенности?	раз в неделю	*Если в процессе анализа приложений могут вноситься изменения (вывод новых версий, добавление нового функционала и т.п.), укажите информацию* *Пример:* *планируются, раз в неделю* *не планируются*
Анализ защищенности веб приложений		
Модель тестирования приложений* ♦ "Черный ящик" - отсутствие учетной записи в приложении и дополнительной информации ♦ "Серый ящик" - наличие учетной записи в приложении и отсутствие дополнительной информации ♦ "Белый ящик" - наличие учетной записи в приложении и дополнительной информации (документация, сведения об окружении, исходый код приложения)	Черный ящик Серый ящик Белый ящик	*Тестирование каждого приложения может проходить как от имени зарегистрированного пользователя, так и анонимно. Укажите модель тестирования для каждого приложения.* *Пример: серый ящик*
Возможен ли процесс самостоятельной регистрации учетных записей в приложениях? В каких приложениях доступна данная возможность?	нет, учетная запись может быть предоставлена	*Пример 1: нет, учетная запись может быть предоставлена* *Пример 2:* *https://computer.store - да* *https://dbofiz.greenbank.ru - нет*
Список ролей, используемых при проведении анализа методом "серого ящика" и их права доступа*	поставщик сотрудник минздрава от региона сотрудник Фонда	*В случае применения модели "серый ящик", укажите роль учетной записи для каждого приложения* *Пример: клиент - минимальные права, оператор - права позволяют обрабатывать конфиденциальную информацию*
Перечень дополнительной информации, которая может быть передана для проведения работ методом "белого ящика" (документация при разработке, инструкции администраторов/операторов/пользователей /документация к API, и т.п.)	Техническое задание на ИС Фонда	*В случае применения модели "белый ящик", укажите перечень информации, которую можете предоставить.* *Пример: документация разработки, исходный код серверной части приложения*
Существует ли возможность, в рамках анализа защищенности методом "белого ящика", развертывания стенда с копией продуктивной версии приложения в инфраструктуре Заказчика или Исполнителя, включая возможности дебагтинга/отладки веб-приложения?	Да	*Пример: да, возможно развертывание стенда с версией, аналогичной продуктивной и наполнением стендовой версии тестовыми данными;* *нет, развертывание стенда не планируется*
** - поля, обязательные для заполнения*		

Информация о приложениях		
Количество мобильных приложений*		*Укажите точное количество приложений, входящих в область анализа* *Пример: 2*
Краткое описание особенностей каждого приложения (предназначение, функциональные особенности, и т.п.)*		*Кратко опишите каждое приложение* *Пример:* *Приложение1: интернет-магазин компьютерной техники* *Приложение 2: система ДБО для физических лиц*
Перечень платформ для каждого приложения*		*Пример:* *Приложение1: Android, iOS* *Приложение2: Android*
URL-адреса на скачивание приложения (при возможности)		*Пример:* *https://apps.apple.com/app/id123* *https://play.google.com/store/apps/details?id=123*
Перечень использованных технологий при разработке приложений и введении их в эксплуатацию (языки программирования, фреймворки, CMS, ОС, СУБД и т.п.)		*Пример: Java, Spring Framevork, AngularJS, Linux, Apache, PostgreSQL*
В каком окружении планируется проведение анализа защищенности приложения: ♦ тестовая инфраструктура ♦ предпродуктивныая ♦ продуктивная		*Анализ может проводиться как на этапе тестирования, так и в продакшене. Укажите, в каком окружении будет проводиться анализ каждого приложения* *Пример: тестовая*
Планируются ли внесение изменений в приложения на протяжении работ по анализу защищенности?		*Если в процессе анализа приложений могут вноситься изменения (вывод новых версий, добавление нового функционала и т.п.), укажите информацию* *Пример:* *планируются, раз в неделю* *не планируются*
Анализ защищенности мобильных приложений		
Модель тестирования приложений* ♦ "Черный ящик" - отсутствие учетной записи в приложении и дополнительной информации ♦ "Серый ящик" - наличие учетной записи в приложении и отсутствие дополнительной информации ♦ "Белый ящик" - наличие учетной записи в приложении и дополнительной информации (документация, сведения об окружении, исходый код приложения)		*Тестирование каждого приложения может проходить как от имени зарегистрированного пользователя, так и анонимно. Укажите модель тестирования для каждого приложения.* *Пример: серый ящик*
Возможен ли процесс самостоятельной регистрации учетных записей в приложениях? В каких приложениях доступна данная возможность?		*Пример 1: нет, учетная запись может быть предоставлена* *Пример 2:* *https://apps.apple.com/app/id123 - да* *https://play.google.com/store/apps/details?id=123 - нет*
Список ролей, используемых при проведении анализа методом "серого ящика" и их права доступа*		*В случае применения модели "серый ящик", укажите роль учетной записи для каждого приложения* *Пример: клиент - минимальные права, оператор - права позволяют обрабатывать конфиденциальную информацию*
Перечень дополнительной информации, которая может быть передана для проведения работ методом "белого ящика" (документация при разработке, инструкции администраторов/операторов/пользователей /документация к API, и т.п.)		*В случае применения модели "белый ящик", укажите перечень информации, которую можете предоставить.* *Пример: документация разработки, исходный код серверной части приложения*

** - поля, обязательные для заполнения*

Анализ защищенности беспроводных сетей		
Количество площадок проведения работ*	1	*Укажите количество площадок, где необходимо провести работы по анализу защищенности беспроводных сетей* *Пример: 2*
Фактические адреса площадок проведения работ*	г. Москва, ул. Маросейка, д. 7/8, стр. 1, этажи 4 - 6	*Укажите адреса площадок* *Пример:* *Площадка 1: 121096, г. Москва, ул. Василисы Кожиной, д. 1, корп. 1, этаж 8, комната 25* *Площадка 2: 123456: г. Москва, ул. Пушкина, д. 4*
Количество беспроводных сетей на каждой площадке (SSID)*	2	*Укажите точное количество беспроводных сетей на каждой площадке* *Пример:* *Площадка 1: 2* *Площадка 2: 1*
Технологии защиты беспроводных сетей:* WEP WPA(2) PSK WPA(2) Enterprise	WPA(2) PSK	*Пример: WPA2 Enterprise*
** - поля, обязательные для заполнения*		

Выявление нестойких паролей		
Количество доменов Active Directory, подлежащих проверке*	1	*Укажите количество доменов Active Directory, учётные записи пользователей которых подвержены выявлению нестойких паролей* *Пример: 2 домена*
Общее количество учетных записей, подлежащих проверке*	97	*Укажите общее количество учетных записей для проверки, как пользовательских, так и сервисных* *Пример: 1000*
Количество проверок	1	*Проверки могут проводиться как единовременно, так и периодически в течение определенного времени. Укажите желаемую периодичность:* *Пример:* *♦ единовременно* *♦ раз в квартал в течение года* *♦ раз в полгода в течение года* *♦ 7 раз в течение года*
Требуется ли подробный отчет о статистике выявленных нестойких паролей	% выявленный паролей по отделам	*Помимо краткого отчета о результатах проведенных проверок Исполнитель может подготовить отчет по статистике выявленных паролей (например, % выявленных паролей по подразделениям). Укажите, требуется ли подробный отчет* *Пример: не требуется*
** - поля, обязательные для заполнения*		

Сканирование уязвимостей		
Количество IP-адресов, подлежащих сканированию*	192	*Укажите количество IP-адресов, подверженных сканированию уязвимостей* *Пример: 200*
Есть ли временные ограничения	Нет ограничений	*Пример:* *♦ Есть, только в рабочее время с 09:00 до 18:00* *♦ Есть, только в рабочие дни* *♦ Нет ограничений*
Есть ли ограничения по интенсивности сетевого трафика		*Пример:* *♦ Есть, не более 20 Мб/с на узел*
** - поля, обязательные для заполнения*		