

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

1. Общие сведения.

1.1. **Заказчик:** Общероссийское общественно-государственное движение детей и молодежи «Движение первых» (далее – Движение Первых).

1.2. **Предмет закупки:** выполнение работ по анализу защищенности веб-приложений Общероссийского общественно-государственного движения детей и молодежи «Движение первых» (далее – работы).

1.3. **Место выполнения работ:** г. Москва, ул. Земляной Вал, д. 50А, стр. 2, эт. / помещ. 16/XVIII, офис Подрядчика – в зависимости от характеристики работ.

1.4. **Срок выполнения работ:** в течение 15 (пятнадцати) календарных дней с даты заключения Договора.

2. Назначение и цели работ:

2.1. Целью выполнения работ является поиск и анализ уязвимостей, и повышение защищенности веб-приложений Заказчика в соответствии с разделом 3 настоящего Технического задания, путем выявления содержащихся в них уязвимостей, анализа выявленных уязвимостей и выработки мер по устранению.

2.2. Для достижения указанной цели должны быть решены следующие задачи:

- Планирование мероприятий по выявлению и анализу уязвимостей;
- Проведение тестирования системы для выявления уязвимостей, в соответствии с Приложением № 1;
- Анализ выявленных в результате тестирования уязвимостей;
- Выработка рекомендаций по устранению выявленных уязвимостей.

2.3. Здесь и далее по тексту настоящего Технического задания под уязвимостью подразумевается любая возможность, позволяющая нарушить работоспособность системы, целостность, доступность или конфиденциальность информации, обрабатываемой системой.

2.4. Конечной целью выполнения работ является демонстрация возможности получения несанкционированного доступа к веб-приложениям Заказчика.

3. Границы работ

3.1. Работы по выявлению и анализу уязвимостей выполняются для веб-приложений (далее – Систем) Движения Первых, представленных в Приложении № 1 к настоящему Техническому заданию.

4. Требования к работам по тестированию

В рамках выполнения Подрядчиком работ по Договору, должны быть проведены все работы, указанные в разделах 4-5 настоящего Технического задания.

4.1. Требования к выполняемым работам.

4.1.1. После подписания Сторонами Договора, до начала выполнения тестирования Систем Подрядчик должен спланировать мероприятия по анализу защищенности веб-приложения (далее – мероприятие), для этого необходимо разработать план тестирования Системы (далее – План тестирования) и посредством электронной почты/путем обмена электронными документами/в письменном виде предоставить Заказчику на согласование.

4.1.2. План тестирования должен включать, в том числе, необходимые подготовительные мероприятия в целях обеспечения безопасности и работоспособности Системы при осуществлении тестирования.

4.1.3. При осуществлении работ Подрядчиком должны быть исключены ситуации, связанные с потерей данных, обрабатываемых в Системе или потерей работоспособности компонентов Системы.

4.1.4. До начала мероприятий должны быть согласованы:

- используемые модели нарушителя;
- степень раскрытия информации и необходимые привилегии для проведения тестирования;
- уровень осведомленности о проведении тестирования сотрудников Заказчика;
- порядок взаимодействия Подрядчика и Заказчика в ходе тестирования;
- временные рамки проведения тестирования;
- обеспечение доступности компонентов тестируемой Системы;
- предоставление специалистам Подрядчика тестовых учетных записей пользователей для каждой из предусмотренных в тестируемой Системе ролей.

4.1.5. При проведении тестирования Подрядчик должен предпринимать все меры предосторожности для сохранения работоспособности тестируемой Системы и компонентов ИТ-инфраструктуры Заказчика.

4.1.6. Состав, порядок и время проведения мероприятий, содержащих риски возникновения деструктивных последствий для тестируемой Системы или ИТ-инфраструктуры Заказчика, определяются и согласуются Подрядчиком и Заказчиком дополнительно письменно или путем обмена электронными документами.

4.2. Требования к проведению тестирования.

4.2.1. После согласования Сторонами Плана тестирования должно быть проведено комплексное тестирование Системы для выявления уязвимостей и последующего анализа выявленных уязвимостей.

4.2.2. Должно быть проведено тестирование всех компонентов Системы, программно-аппаратного окружения, включая, но не ограничиваясь следующим: сетевое взаимодействие, настройки ОС, источники данных, хранилища информации, механизмы авторизации, среда передачи данных.

5. Методология выполнения работ

5.1. Анализ защищенности проводится по методике Подрядчика (предоставляется по запросу Заказчика) в соответствии со следующими международными стандартами и практиками:

- Penetration Testing Execution Standard (PTES);
- NIST Special Publication 800-115, Technical Guide to Information Security Testing and Assessment;
- Open-Source Security Testing Methodology Manual (OSSTMM);
- Information Systems Security Assessment Framework (ISSAF);
- Web Application Security Consortium (WASC) Threat Classification;
- Open Web Application Security Project (OWASP) Testing Guide;
- Стандарты Center for Internet Security (CIS);
- Common Vulnerability Scoring System v3.0 (CVSS v3.0).

5.2. В процессе тестирования Подрядчик уведомляет Заказчика о возникающих ситуациях, препятствующих выполнению работ. Необходимые для устранения указанных ситуаций сроки и меры определяются и согласуются Подрядчиком и Заказчиком дополнительно письменно или путем обмена электронными документами.

5.3. Подрядчик должен учитывать возможность корректировки реализуемой им методики тестирования Системы и последующего анализа уязвимостей с учетом собственного опыта и наработок, а также с учетом промежуточных результатов тестирования и особенностей исследуемой Системы Заказчика.

5.4. Для решения поставленных задач Подрядчик выполняет работы для Заказчика в соответствии с Таблицей № 1.

Таблица № 1

№ п/п	Виды и порядок выполнения работ	Перечень работ	Необходимые ресурсы	Срок выполнения
1	Сбор и анализ документации Систем	1. Анализ архитектуры Систем 2. Уточнение типа злоумышленника 3. Описание точек входа в Систему 4. Изучение особенностей конфигурации 5. Разработка векторов атаки	Документация и описание компонентов Систем	2 (два) календарных дня с даты подписания договора
2	Анализ защищенности компонентов Систем (методом «серого ящика»)	Проведение тестирования и анализа защищенности по методике Подрядчика, в соответствии с утвержденным планом проведения анализа защищенности	Учетные записи с различными привилегиями в Системе в соответствии с выбранной моделью злоумышленника	10 (десять) календарных дней с момента завершения сбора и анализа документации систем
3	Подготовка отчета	Подготовка и согласование итогового отчета в соответствии с формой, описанной в методике Подрядчика	—	3 (три) календарных дня с момента завершения анализа защищенности компонентов Систем

5.5. Работы, перечисленные в Таблице № 1, включают в себя следующие виды работ:

5.5.1. Сбор и анализ информации о Системе:

- изучение и анализ архитектуры;
- уточнение типа злоумышленников;
- описание точек входа;
- изучение особенностей конфигурации;
- разработка векторов атаки.

5.5.2. Проведение анализа защищенности:

- обнаружение ошибок исполнения;
- анализ защищенности канала передачи данных;

- тестирование механизма создания и управления пользователями;
- тестирование механизма аутентификации;
- тестирование механизма разграничения доступа (авторизации);
- тестирование механизма валидации пользовательских данных;
- тестирование механизма управления сессиями;
- тестирование бизнес-логики;
- поиск векторов атаки на пользователей приложения;
- применение инструментов автоматизированного анализа.

5.5.3. Подготовка отчета для соответствующей информационной системы:

- общая информация;
- экспертная оценка текущего уровня защищенности;
- перечень обнаруженных уязвимостей;
- общие рекомендации по повышению уровня защищенности;
- подробная информация о найденных уязвимостях, включая описание, уровень опасности, место обнаружения, пример эксплуатации и рекомендации по устранению.

5.6. Поиск уязвимостей осуществляется последовательно в автоматическом режиме и ручном режимах.

5.7. Автоматический поиск уязвимостей осуществляется с использованием сертифицированных ФСТЭК России средств анализа защищенности. После автоматизированного поиска уязвимостей проводится ручной поиск, включающий в себя проверки по методикам, указанным в пункте 5.1.

5.8. Работы, перечисленные в Таблице № 1 должны быть выполнены для всех Систем, указанных в Приложении № 1.

6. Требования к подготовке отчета

6.1. По итогу выполнения тестирования Подрядчик должен подготовить отчет соответствующей Системы.

6.2. Должна быть проведена систематизация результатов тестирования, в том числе, проведено описание использованных методик и хода тестирования, выявленных уязвимостей, их классификация и оценка критичности. Оценка уровня риска уязвимостей должна проводиться на основе описанных методик.

6.3. Должно быть проведено описание векторов реализованных атак, методов и ограничений эксплуатации выявленных уязвимостей, и возможных последствий реализации выявленных уязвимостей.

7. Требования к выработке рекомендаций

7.1. По итогу выполнения анализа результатов тестирования Подрядчик должен выработать рекомендации по устранению выявленных уязвимостей.

7.2. Должен быть разработан план мероприятий, обеспечивающий нейтрализацию выявленных уязвимостей с учетом присвоенного им уровня риска, а также список организационных и технических мер, необходимых для обеспечения защищенности Системы.

7.3. В том числе, должны быть разработаны подробные технические рекомендации:

- по нейтрализации выявленных уязвимостей;
- по изменению конфигурации и настроек программно-аппаратного обеспечения Системы, ее окружения;
- по оптимизации параметров, состава и структуры используемой системы защиты информации.

7.4. Также, при необходимости, должны быть разработаны:

- требования и рекомендации по организации процессов безопасной разработки программного кода Системы;
- предложения по минимизации возможных последствий атак;
- предложения по организации деятельности Заказчика с целью минимизации уязвимостей Системы.

8. Требования к Подрядчику

8.1. Подрядчик должен обладать действующей лицензией Федеральной службы по техническому и экспортному контролю на деятельность по технической защите конфиденциальной информации и соответствовать требованиям Федерального закона от 04.05.2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности», постановления Правительства Российской Федерации от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».

8.2. Специалисты Подрядчика, привлеченные к выполнению работ в рамках настоящего технического задания, должны иметь квалификацию в области защиты информации, подтвержденную сертификатами государственного образца и/или соответствующими международными сертификатами OSCP.

9. Состав отчетной документации

9.1. В соответствии с целями раздела 2 и раздела 4 настоящего Технического задания необходимые мероприятия (проводимые работы) и соответствующая отчетная документация определены в Таблице № 2.

Таблица №2

№ п/п	Наименование работ	Отчетная документация
1	Планирование мероприятий по выявлению и анализу уязвимостей	План тестирования и протокол согласования подготовки тестирования системы (по требованиям пп. 4.1)
2	Тестирование системы, анализ результатов тестирования (выявление и анализ выявленных в результате тестирования уязвимостей)	Отчет о выявлении и анализе уязвимостей системы (по требованиям разделов 4-5)
3	Выработка рекомендаций по устранению выявленных уязвимостей	Отчет о выработанных рекомендациях по устранению выявленных уязвимостей и обеспечению защищенности системы (по требованиям п. 7)

10. Конфиденциальность

10.1. При взаимодействии между Сторонами подписывается соглашение о неразглашении информации.

10.2. Стороны в полной мере осознают критичность информации, как исходных данных, так и результатов услуг.

10.3. В ходе выполнения работ специалисты Подрядчика не предпринимают каких-либо действий, которые могут привести к уничтожению или блокировке информационных активов Заказчика.

11. Требования к оформлению отчетных документов

11.1. Технические требования, предъявляемые к отчетной документации.

Отчетная документация представляется Заказчику на бумажном носителе формата А4 (допускается формат А3 по согласованию с Заказчиком) и в электронном виде на оптическом

носителе (USB-накопитель с файлами в формате Microsoft Word) в количестве, предусмотренном договором.

11.2. Требования к оформлению: страницы текста отчета (на одной стороне листа белой бумаги) и включенные в отчет иллюстрации и таблицы должны соответствовать формату А4, через полтора интервала. Цвет шрифта должен быть черным Times New Roman, высота букв, цифр и других знаков – 1.8 мм (кегель 12 pt), размеры полей: правое – 10 мм, верхнее и нижнее – 20 мм, левое – 30 мм. Для подготовки отчетных материалов следует руководствоваться следующими нормами – 1 п.л. составляет 16 страниц машинописного текста без учета иллюстраций, схем и рисунков.

Отчет должен быть прошит или сброшюрован.

Страницы Отчета должны быть пронумерованы.

Если отчет больше 500 (пятисот) листов, документ должен быть разделен на несколько томов, при этом каждый том не может быть более 500 (пятисот) листов.

Отчет должен быть прошит и скреплен печатью (при наличии) и подписью Подрядчика.

11.3. Структурными элементами Отчета о выполненных работах (оказанных услугах) должны являться:

- титульный лист (оформляется в соответствии с Приложением № 2 к настоящему Техническому заданию);
- оглавление;
- нормативные ссылки;
- определения;
- обозначения и сокращения;
- основная часть;
- приложения (при наличии).

На титульном листе должны быть указаны следующие сведения:

- наименование Подрядчика тела по договору;
- наименование Отчета;
- подпись с указанием должности, фамилии и инициалов представителя Подрядчика по договору, подписавшего Отчет;
- место и дата составления Отчета.

11.4. Если Отчет состоит из двух и более частей, то каждая часть должна иметь свой Титульный лист, соответствующий Титульному листу первой части и содержащий сведения, относящиеся к данной части.

11.5. Оглавление должно включать наименование всех разделов, подразделов, пунктов (если они имеют наименование) и наименование приложений с указанием номеров страниц, с которых начинаются соответствующие элементы отчета о выполненных работах (оказанных услугах).

11.6. При составлении Отчета, состоящего из двух и более частей, в каждую часть Отчета должно быть включено оглавление. При этом в первой части Отчета должно содержаться оглавление всего Отчета с указанием номеров частей, в последующих – только оглавление соответствующей части. Допускается в первой части Отчета вместо оглавления последующих частей указывать только их наименование (номер).

11.7. В приложения рекомендуется включать документы и (или) материалы, связанные с выполнением работ (оказания услуг), которые по каким-либо причинам не могут быть включены в основную часть Отчета или которые в соответствии с требованиями технического задания должны быть представлены в виде отдельно указанных документов.

11.8. Финансовый отчет

11.8.1. Финансовый отчет является отчетным документом, предоставляемым Подрядчиком договора с целью подтверждения объема расходов и величины дохода Подрядчика.

11.8.2. Финансовый отчет является неотъемлемой частью договоров между Подрядчиком договора и Заказчиком. Финансовый отчет формируется по форме, предусмотренной договором.

11.8.3. Наименование работ и услуг, указываемых в финансовом отчете, должно строго соответствовать спецификации, к договору по которому составляется финансовый отчет.

11.8.4. Финансовый отчет должен включать в себя информацию о понесенных Подрядчиком затратах при исполнении договора.

11.8.5. Подтверждением понесенных Подрядчиком затрат на услуги соисполнителей являются скан-копии прямых договоров и актов выполненных работ, оказанных услуг с подрядчиками.

11.8.6. В случае, если исполнение договора осуществляется собственными силами, Подрядчику необходимо предоставить бухгалтерские справки, содержащие информацию, подтверждающую осуществление расходов (в том числе, но не ограничиваясь: приказы о создании рабочей группы, таблицы учета рабочего времени, выписка из штатного расписания, расчет расходов на оплату труда с отчислениями, ведомость наличия основных средств, ведомость списания материалов, сырья, ведомость раздачи сувенирной продукции).

11.8.7. Помимо фактически понесенных Подрядчиком затрат на услуги сторонних организаций, а также прямых и накладных расходов, финансовый отчет должен содержать информацию о вознаграждении Подрядчика.

11.8.8. Финансовый отчет с приложенными обоснованиями предоставляется Подрядчиком Заказчику на бумажном носителе в одном экземпляре, прошитым и подписанным руководителем или должностным лицом, уполномоченным действовать от лица Подрядчика, и заверенным печатью Подрядчика.

11.8.9. Заказчик проверяет предоставленный Подрядчиком финансовый отчет в течение периода, указанного в договоре. Если Заказчик не согласен с представленным ему финансовым отчетом, Подрядчик должен учесть обоснованные замечания Заказчика и представить финансовый отчет повторно.

Подписи сторон:

Заказчик:

Подрядчик:

_____/_____
М.П.

_____/_____
М.П.

Границы работ по выявлению уязвимостей в Движении Первых

№ п/п	Наименование веб-приложения	Расположение веб-приложения
1	Сайт Елкажеланий.рф	https://елкажеланий.рф/
2	Проектный модуль Движения Первых	https://projects.pervye.ru/

Подписи сторон:

Заказчик:

Подрядчик:

_____/_____
М.П.

_____/_____
М.П.

ФОРМЫ ТИТУЛЬНОГО ЛИСТА И ОБЛОЖКИ ВНЕШНЕГО НОСИТЕЛЯ
С ЭЛЕКТРОННОЙ ВЕРСИЕЙ ОТЧЕТА ОБ ИСПОЛНЕНИИ УСЛОВИЙ ДОГОВОРА
И ВЫПОЛНЕННЫХ РАБОТАХ

1. ФОРМА ТИТУЛЬНОГО ЛИСТА

**ОБЩЕРОССИЙСКОЕ ОБЩЕСТВЕННО-ГОСУДАРСТВЕННОЕ ДВИЖЕНИЕ ДЕТЕЙ И
МОЛОДЕЖИ «ДВИЖЕНИЕ ПЕРВЫХ»**

ОТЧЕТ

СОГЛАСОВАНО:

УТВЕРЖДЕНО:

*Должность руководителя инициатора
закупки*

_____/_____/

_____/ **ФИО** /

ОТЧЕТ

об исполнении условий Договора/аналитический отчет

от «____» _____ 20__ г. № _____

по договору от «____» _____ 20__ г. № _____

Предмет: «_____»

Указывается предмет в соответствии с заключенным договором

Подрядчик:

*Указывается полное наименование Подрядчика в соответствии с заключенным
договором*

от Заказчика

от Подрядчика

Инициатор закупки

Должность инициатора закупки

должность руководителя Подрядчика

_____/ **ФИО** /

_____/ **ФИО** /

г. _____, 20__ г.

2. ОБЛОЖКА ВНЕШНЕГО НОСИТЕЛЯ:

ЭЛЕКТРОННАЯ ВЕРСИЯ ОТЧЕТА ПО ДОГОВОРУ от « <u> </u> » <u> </u> 20 № <u> </u> / /	
ПРЕДМЕТ ДОГОВОРА:	
ПОДРЯДЧИК:	<i>Должность подписанта от</i> <i>Подрядчика:</i> _____/И.О.Фамилия М.П.

3. ФОРМА ДЛЯ СКРЕПЛЕНИЯ ПРОШИТОГО ОТЧЕТА

Наименование Подрядчика	Прошито, пронумеровано и скреплено печатью _____ листов Должность _____ ФИО « <u> </u> » _____ 202 <u> </u> г.
-------------------------	---

Формы согласованы

Подписи Сторон:

Заказчик:

М.П.

Подрядчик:

Должность

_____/_____
М.П.