# Приложение № 1

|  |  |  |
| --- | --- | --- |
|  | **УТВЕРЖДАЮ:** | |
|  | |
|  | |
| *(должность начальника подразделения – Инициатора)* | |
|  | |
| *(Ф. И. О. начальника)* | |
|  | |
| *(подпись)* | |
|  | |
|  | | |
| **ТЕХНИЧЕСКОЕ ЗАДАНИЕ**  **для**  **договора возмездного оказания услуг по Обеспечению информационной безопасности корпоративного сайта расположенного в глобальной компьютерной сети Интернет** | | |
|  | | |
| Требования к предмету закупки | | |
|  | | |
| Общие требования к качеству | | |
| Исполнитель оказывает услуги по обеспечению информационной безопасности корпоративного сайта Заказчика (далее – сайт) в глобальной компьютерной сети интернет на основании заявок Заказчика и сообщений системы мониторинга, в объеме, описанном в п.1.6 настоящего Технического задания. | | |
|  | | |
|  | | |
| Требования к техническим характеристикам | | |
| Технические параметры корпоративного сайта:  Система администрирования сайта – «1С-Битрикс: Управление сайтом».  Доступ к системе защищен на уровне программного обеспечения сервера. Авторизационные данные предоставляются Заказчиком после заключения договора.  Электронный адрес корпоративного сайта Заказчика в глобальной сети интернет: [www.pulkovoairport.ru](http://www.pulkovoairport.ru) | | |
|  | | |
|  | | |
| Требования к размерам (заполняется для товаров) | | |
| Отсутствуют | | |
|  | | |
|  | | |
| Требования к упаковке (заполняется для товаров) | | |
| Отсутствуют | | |
|  | | |
|  | | |
| Требования к отгрузке (заполняется для товаров) | | |
| Отсутствуют | | |
|  | | |
|  | | |
| Термины, определения и сокращения  |  |  | | --- | --- | | Термин | Определение | | Централизованный мониторинг | Информационная система, обеспечивающая сбор, хранение, обработку, агрегацию и представление значений метрик, а также генерацию и доставку алертов/уведомлений об аварийных и предаварийных событиях | | СПО | Специальное программное обеспечение автоматизированных информационных систем, установленное и выполняющееся на серверах с предварительно настроенным БПО, поставляемое непосредственно разработчиками веб-сайта | | БПО (ОПО) | Базовое (основное) программное обеспечение сервера, включающее базовую операционную систему, совместимое с ней программное обеспечение СУБД, WEB серверов, подсистемы управления сетевым и системным доступом, а также прочее ПО, относящееся к дистрибутивам непосредственно базовой операционной системы, либо сторонним бинарно-совместимым дистрибутивам | | ОС | Операционная система, в которой непосредственно осуществляется выполнение БПО, СПО, и компонентов веб-сайта. Является гостевой, применительно к системе виртуализации. | | ВЕБ-САЙТ | Информационная система, выполненная в виде веб-приложения | | OpenSource | Программное обеспечение с открытым исходным кодом | | Сервер (виртуальный сервер) | Совокупность аппаратных или виртуализированных вычислительных ресурсов, обеспечивающих выполнение операционной системы, БПО и СПО | | Гипервизор | компьютерное программное обеспечение, микропрограммное обеспечение или аппаратное обеспечение, которое создает и запускает виртуальные машины. | | Алерт (алертинг) | Сообщение или уведомление от системы централизованного мониторинга, генерируемое при получении метрик, выходящих за пределы нормы, для наблюдаемого объекта. Имеет целью уведомление сотрудников Исполнителя и Заказчика о нештатном состоянии компонентов технологической инфраструктуры | | СУБД | Система управления базами данных | | ПО | Программное обеспечение | | НШС | Нештатная ситуация | | База данных общеизвестных уязвимостей информационной безопасности (CVE) | CVE (англ. Common Vulnerabilities and Exposures) — база данных общеизвестных уязвимостей информационной безопасности. Каждой уязвимости присваивается идентификационный номер вида CVE-год-номер, описание и ряд общедоступных ссылок с описанием | | Инцидент | Любое событие, нарушающее нормальную работу веб-сайта, в том числе ведущее или способное привести к остановке или снижению качества его работы | | Обращение | Уведомление Исполнителя Пользователем об инциденте, возникшем при функционировании систем веб-сайта для организации оказания государственных услуг | | Недопустимое событие | Событие, возникающее в результате действий злоумышленников и делающее невозможным достижение операционных и стратегических целей или приводящее к длительному нарушению основной деятельности организации. | | Brute Force | Атака методом полного перебора | | SQL | Structured Query Language - язык структурированных запросов | | XML | eXtensible Markup Language - расширяемый язык разметки. Используется для хранения и передачи данных | | LFI | Local File Inclusion - подключения локальных файлов с выводом для чтения на стороне сервера | | RFI | Remote file include - удалённое выполнение кода на сервере. | | RCE | Remote code execution - удалённое внедрение кода на сервере | | XSS | Cross-Site Scripting - межсайтовый скриптинг | | SMTP | Simple Mail Transfer Protocol - простой протокол передачи почты | | SSI | Server Side Includes - включения на стороне сервера | | LDAP | Lightweight Directory Access Protocol - протокол прикладного уровня для доступа к службе каталогов | | XQuery | язык запросов и функциональный язык программирования, разработанный для обработки данных в формате XML | | HTTP | HyperText Transfer Protocol – протокол передачи гипертекста | | CSRF | Cross-site request forgery - межсайтовая подделка запроса |  Количество товара, объем работ, услуг | | |
| Функциональные доработки веб-сайта Состав услуг по обеспечению информационной безопасности корпоративного сайта на основании заявок Заказчика и уведомлений системы мониторинга. Осуществление обработки и выполнения заявок Заказчика по согласованию с Заказчиком, включая обеспечение защиты сайта от DoS и DDoS-атак, защиты от атак на веб-приложения. Проведение мониторинга работоспособности сайта и устранение неполадок в случае их возникновения.  Услуги оказываются на основании выявленных Исполнителем Инцидентов либо на основании Заявок Заказчика, направляемых на «горячую линию» Исполнителя (по телефону, электронной почте, чат в телеграмм, через систему управления проектами). Срок выполнения Заявок Заказчика определяется по согласованию с подрядчиком.  Стороны фиксируют в договоре рабочие часы (например, с 08:30 до 17:30) или другой интервал времени, не менее 8 рабочих часов в день (в зависимости от договоренностей, зафиксированных в договоре), в которые Исполнитель с понедельника по пятницу исполняет виды заявок: «стандартная заявка» и «срочная заявка».  Стороны фиксируют, что заявки вида «Заявка, связанная с нарушением штатного функционирования сайта» и их исправления направляются и исполняются в графике 24/7. Исполнитель должен быть доступен круглосуточно семь дней в неделю, в том числе в нерабочее время, и иметь возможность выполнить срочные заявки, в случае необходимости.   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **№** | **Вид заявки** | **Состав Заявки** | **Срок реагирования** | **Максимально допустимый срок выполнения** | | 1 | Стандартная заявка | Выполнение рекомендаций и устранение замечаний, направленных Заказчиком. | 2 часа | По согласованию с Заказчиком | | 2 | Срочная заявка | Выполнение срочных рекомендаций и исправлений, полученных от регуляторов | 30 минут | По согласованию с Заказчиком | | 3 | Заявка, связанная с нарушением штатного функционирования сайта | Любой состав работ, связанных с нарушением штатного функционирования сайта как по внутренним причинам, так и в результате внешнего вмешательства. | Исполнитель должен известить ответственных лиц Заказчика в течение не более 5 минут со времени выявления штатного функционирования сайта.  Исполнитель должен самостоятельно сформировать заявку, известить заказчика не позднее чем через 15 минут с момента выявления проблем штатного функционирования сайта и действовать согласно разделу 1.7.6. Настоящего ТЗ. | Всплывающее окно (pop-up) о технических работах на сайте должно появиться в течение 5 минут после выявления нарушения штатного функционирования сайта.  Срок восстановлениия работоспособности по согласованию с Заказчиком. |  * + 1. Требования к обеспечению отказоустойчивости, безопасности, производительности, масштабируемости инфраструктуры.   В рамках настоящего Технического Задания Исполнитель должен оказывать услуги по технической поддержке технологической инфраструктуры Заказчика, используемой для функционирования веб-сайта (в границах ответственности Исполнителя и с учетом ограничений, накладываемых провайдерами облачных услуг) в целях улучшения следующих показателей работы технологической инфраструктуры и веб-сайта, располагающегося на ней:   1. отказоустойчивость; 2. безопасность; 3. производительность; 4. масштабируемость.   Для этого Исполнитель:   1. проводит аудит инфраструктуры и сервисов, передаваемых ему на сопровождение; 2. разворачивает средства централизованного мониторинга на единой технологии для контроля функционирования серверов и процессов сетевого взаимодействия, систем безопасности функционирования серверов, систем виртуализации; 3. осуществляет мониторинг событий информационной безопасности и проводит работы по настройке операционных систем 4. собирает и анализирует тревожные сообщения от системы мониторинга, заблаговременно предупреждая развитие аварийных ситуаций (при наличии объективной возможности); 5. проводит настройки (в случае необходимости - обновление) БПО серверов для оптимизации параметров работы; 6. проводит настройки (в случае необходимости - обновление) БПО серверов виртуализации для оптимизации параметров работы.   Проводит работы по задачам:   1. проводит техническое расследование инцидентов, зафиксированных через средства централизованного мониторинга и/или по обращениям Заказчика, 2. в случае наличия технической возможности, восстанавливает работоспособность систем в кратчайшие сроки; 3. ежемесячно составляет отчет по инцидентам (если имеются) и отчет по сопровождению, а также отчет по результатам мониторинга информационной безопасности виртуальных серверов 4. консультирует Заказчика и, при необходимости, подрядчиков, обслуживающих ВЕБ-САЙТ, в части эксплуатации серверного БПО, ПО виртуализации, ПО СУБД и другого серверного ПО; 5. Консультирует Заказчика по вопросам эксплуатации Positive Technologies Application Firewall, защищающем веб-сайт. 6. Консультирует Заказчика по вопросам эксплуатации средств защиты веб-сайта от DoS и DDoS атак (например Qrator).    * 1. **Требования к аудиту инфраструктуры веб-сайта.**   Исполнитель в рамках аудита инфраструктуры веб-сайта оказывает следующие виды услуг (если применимо):   1. Инвентаризация виртуальных серверов. 2. Инвентаризация физических серверов системы виртуализации, сетевого оборудования, систем хранения данных. 3. Установка агентов централизованного мониторинга и алертинга на сервера, подключение к централизованной системе мониторинга, настройка постоянного сбора метрик. 4. Аудит ОС, СПО и БПО и версионирование, включая проверку возможности технической поддержки/установки обновлений безопасности. 5. Проверка наличия цифровых подписей репозиториев. 6. Проверка периодичности установки обновлений. 7. Проверка используемых SSL сертификатов и постановка их на мониторинг/контроль истечения. 8. Проверка наличия локальных резервных копий. 9. Сбор информации о фактической сетевой активности, документирование схем сетевой связности. 10. Описание имеющихся СУБД (тип, расположение, резервные копии, объем, нагрузка). 11. Анализ использования виртуальных и физических вычислительных ресурсов, выявление перегруженных серверов. 12. Описание выявленных по результатам аудита проблем, перечень рекомендаций по их устранению и оптимизации функционирования. Перечень рекомендаций по устранению выявленных проблем и оптимизации функционирования систем должен содержать список изменений в настройках БПО.   Требуемые виртуальные ресурсы и прочие покупные требуемые товарно-материальные ценности обеспечиваются Заказчиком.   * + 1. **Требования к качеству и безопасности разработки.**   Исполнитель обязуется организовать процесс верификации разработки с точки зрения безопасности:   1. Выполнение мероприятий по ИБ, которые относятся к циклу разработки ПО (проверка разрабатываемого кода на наличие уязвимостей и т.п.) и сотрудникам (управление доступами, система аутентификации и авторизации и т.д.)   **1.7.5. Требования к контролю и обеспечению информационной безопасности.**  Исполнитель осуществляет контроль безопасности веб-сайта путем анализа уязвимостей на уровне прикладного ПО, включая следующий состав работ, при обнаружении уязвимостей осуществляется их устранение (в границах ответственности Исполнителя):  В процессе выполнения работ должна осуществляться проверка наличия следующих уязвимостей:   * некорректная обработка пользовательского ввода, которая позволяет проводить следующие виды атак:   + внедрение операторов языка SQL (англ. SQL injection), в том числе межмодульное (англ. Second order);   + межсайтовое выполнение сценариев (Cross-Site Scripting);   + подделка межсайтового запроса (Cross-Site Request Forgery);   + включение локальных и удаленных файлов (англ. LFI/RFI/RCE);   + внедрение кода на языке, интерпретируемом на стороне клиента (англ. XSS),  в том числе межмодульное (англ. Stored) и клиентское (англ. DOM-based);   + внедрение команд, интерпретируемых средой выполнения (англ. Eval injection);   + внедрение команд, интерпретируемых ОС сервера (англ. OS command injection);   + внедрение SMTP-команд;   + внедрение директив SSI;   + внедрение конструкций языка запросов LDAP;   + внедрение конструкций языка запросов XPath/XQuery;   + внедрение разметки на языке XML;   + внедрение заголовков (Header Injection), в том числе позволяющие разделить HTTP-ответ;   + подключение внешних XML-сущностей (англ. XML External Entity);   + прочие атаки, целью которых является выполнение кода на стороне сервера;   + атака на переполнение буфера применяемых программных и программно-аппаратных компонентов ИС; * небезопасная реализация загрузки пользовательских файлов на сервер (англ. Unrestricted Upload of File with Dangerous Type); * отсутствие проверки или некорректная проверка привилегий пользователя при доступе к закрытым функциям или ресурсам (англ. Insufficient authorization); * ошибки в протоколе проверки подлинности пользователей (англ. Insufficient authentication); * уязвимости в процедуре восстановления доступа при утере учетных данных  (англ. Insufficient password recovery); * уязвимости в организации безопасного соединения (англ. Insufficient Transport Layer Protection); * уязвимости, связанные с некорректным управлением сеансами (англ. Insufficient Session Expiration); * возможность несанкционированного выполнения запросов от имени пользователей  (англ. CSRF); * возможность вызвать отказ в обслуживании (англ. Denial of Service) без применения методов валовой посылки запросов; * некорректная обработка исключительных ситуаций, приводящая к утечке информации  о приложении (англ. Information Leakage); * выявление общеизвестных уязвимостей в ИС; * выявление ошибок конфигурации в ИС; * поиск уязвимостей в ИС, связанных с некорректной обработкой входных данных  от пользователей; * выявление уязвимостей, связанных с логикой работы ИС; * выявление других свойств ИС, негативно влияющих на безопасность (hardening); * прочие ошибки, позволяющие изменить логику работы ИС.   Исполнитель осуществляет контроль безопасности веб-сайта путем анализа уязвимостей на уровне исходного кода, включая следующий состав работ, при обнаружении уязвимостей осуществляется их устранение (в границах ответственности Исполнителя):   * Анализ архитектурно-технологических решений с целью выявления архитектурных уязвимостей; * Анализ защищенности серверного API; * Анализ механизмов хранения данных; * Анализ механизмов самозащиты приложения; * Анализ защищенности канала передачи данных; * Поиск уязвимостей в приложении, связанных с некорректной обработкой входных данных; * Анализ безопасности используемых сторонних компонентов; * Проверка на наличие избыточной функциональности; * Выявление недекларированных возможностей; * Проведение анализа безопасности исходного кода системы автоматизированными средствами и «ручным образом» (с последующей валидацией в прикладном приложении).   Исполнитель, при обслуживании веб-приложения и получении доступа к персональным данным, обязуется без письменного разрешения Заказчика не осуществлять действий по обработке персональных данных, включая: копирование, передачу третьим лицам и т.д.  Исполнитель, при необходимости работы с веб-приложением за границами инфраструктуры Заказчика (например, при необходимости создания контуров разработки и(или) тестирования на стороне Исполнителя) стремится, при наличии объективной возможности, к отсутствию в базе данных приложения персональных данных.  Исполнитель обязуется соблюдать требования Заказчика в области защиты персональных данных (при условии предоставления Заказчиком таковых требований), включая: технические условия на подключение, политики и регламенты в области защиты персональных данных.  При условии внедрения Заказчиком средств защиты персональных данных (обрабатываемых веб-приложением), напрямую размещенных на той же виртуальной машине, что и веб-приложение, Исполнитель обязуется обеспечивать функционирование таковых средств защиты персональных данных.  Исполнитель обязуется проявлять (все зависящие от него) разумные и общепринятые меры должной осмотрительности в части информационной безопасности для недопущения утечки персональных данных.  Исполнитель не несет ответственности за недочеты, имеющиеся в коде на момент передачи его Исполнителю при старте работ. | | |
| 1.7.6. **Требования по реагированию на инциденты.**  При возникновении проблем в работоспособности сайта вследствие воздействия инцидентов перед выполнением работ по восстановлению необходимо в кратчайшее возможные сроки выполнить следующие шаги:   * уведомить определенный круг лиц заказчика, максимально быстрым способом, о возникшем инциденте, убедившись, что с данной информацией заказчик ознакомился; * сохранить все лог-файлы, связанные с данным инцидентом; * сохранить образ сайта с наличием инцидента; * выполнить работы по восстановлению работоспособности сайта; * после восстановления провести краткий анализ причин возникновения инцидента; * предоставить Заказчику все материалы по инциденту, включая собственные выводы по его возникновению.   1.7.7. **Требования к централизованному мониторингу.**  Система Мониторинга состояния СПО и БПО должен отвечать следующим условиям:   * должна охватывать метрики всех серверов веб-сайта, средств защиты информации, всего оборудования и систем виртуализации, находящихся в зоне ответственности Исполнителя; * должна предоставлять инструменты для анализа и отображения собранных метрик в едином интерфейсе; * должна обеспечивать возможность графического отображения произвольного сочетания метрик; * должна обеспечить доставку тревожных сообщений, как минимум, двумя различными способами.   Список аккумулируемых метрик должен соответствовать списку ниже и может быть расширен по согласованию с заказчиком.  Исполнитель настраивает мониторинг и рассылку уведомлений в случае подмены файлов на веб-сайте.  **ТРЕБОВАНИЯ К МЕТРИКАМ ИС МОНИТОРИНГА (при наличии возможности в инфраструктуре Заказчика)**  Группы метрик мониторинга, которые должны обеспечивать контроль степени использования ресурсных емкостей и состояния работы БПО и СПО, собираются круглосуточно в автоматическом режиме с целью контроля превышения пороговых значений.   |  |  | | --- | --- | | **№ п/п** | **Описание групп метрик мониторинга** | | 1. | Использование центральных процессоров и процессорного времени системы в разрезе ядер, аппаратных и программных прерываний, времени использования пространства ядра и пользовательского пространства, переключений контекстов. | | 2. | Использование оперативной памяти в разрезе пространств памяти, занятых под дисковый и системный кеш, буферы, активные и неактивные страницы, заблокированные и используемые для подкачки области, использование областей разделяемой памяти и использование файлов подкачки | | 3. | Использование дисковых подсистем в разрезе блочных устройств, включая объемы записи и чтения в операциях в секунду и в количестве переданных и принятых байт, а также время отклика дисковой подсистемы в разрезе обращений к каждому диску, использование индексных дескрипторов файловых систем и использование дискового пространства в байтах и процентах, включая использование дисковых подсистем | | 4. | Использование сетевых интерфейсов, включая объемы переданных и принятых данных в байтах в секунду и пакетах в секунду в разрезе сетевых интерфейсов | | 5. | Использование системных сокетов, количества соединений по протоколам TCP или UDP, включая количество перепосылов, запросов на установление сетевых соединений, ошибок доставки, ошибок подтверждения доставки данных, количество находящихся в ожидании соединений, задействование памяти сетевых буферов и переполнения сетевых буферов | | 6. | Количество исполняемых процессов и тредов в системе, средние показатели общей загрузки системы, состояние процессов в разрезе нахождения их в режимах исполнения, ожидания исполнения, остановки, прерываемого и непрерываемого сна | | 7. | Мониторинг сетевой доступности приложений на уровне TCP (наличие и время ответа на соединение экземпляром СПО, СУБД или иным сетевым компонентом прикладного ПО). | | 8. | Мониторинг сетевой доступности внутренних приложений на по протоколу http(https).  Наличие, код и время ответа. | | 9. | Метрики времени отклика приложений СПО на валидные запросы по протоколам HTTP с указанием кастомизированного тела запроса, времени на установление соединения, передачу данных и полного времени выполнения запроса. | | 10. | Метрики использования отслеживаемых ядром сетевых соединений и передачи трафика через сетевые фильтры в байтах и пакетах | | 12. | Метрики доступности удаленных хостов связанных подсистем, включая сетевую задержку в обе стороны, процент потерь пакетов, минимальное и максимальное время ответа, количество переданных и принятых пакетов и среднее время ответа удаленной подсистемы | | | |
|  | | |
| Место, сроки (периоды), иные условия закупки | | |
|  | | |
| Место поставки товара, выполнения работ, оказания услуг (указывается, если отличается от места нахождения Общества) | | |
| Услуги по сопровождению корпоративного сайта оказываются удаленно. | | |
|  | | |
|  | | |
| Сроки (периоды, стадии) поставки товара, выполнения работ, оказания услуг | | |
| Исполнитель оказывает услуги в течение 36 месяцев с даты заключения договора. | | |
|  | | |
|  | | |
| Иные условия поставки товара, выполнения работ, оказания услуг | | |
| Готовность подрядчика обеспечить постоянную работоспособность сайта, максимальное число часов недоступности сайта – не более 12 часов в год. | | |
|  | | |
|  | | |
| Требования к потенциальному поставщику | | |
|  | |  |
| наличие прав на осуществление определенных действий (деятельности): | |  |
|  | |  |
|  | |  |
| иные; Подтверждение наличия постоянных сотрудников на каждой позиции, превышающее минимальное значение:   * Специалист со знанием (минимум 1 человек): * сетей и сетевых технологий; * Linux систем; * систем виртуализации (Vmware); * Систем мониторинга и визуализации; * nginx\apache; * Positive Technologies Application Firewall; * Qrator.   Должны быть предоставлены копии трудовых договоров/договоров ГПХ/выписок  В соответствии с законодательством (Федеральный закон от 04.05.2011 г. № 99-ФЗ, подпунктом 5 пункта 1 статьи 12 «О лицензировании отдельных видов деятельности», постановлением Правительства Российской Федерации от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»), Указом Президента №250, разработанными Минцифры требованиями, Исполнитель должен обладать:  Действующей лицензией Федеральной службы по техническому и экспортному контролю России на деятельность по технической защите конфиденциальной информации, включая:  «б» услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации;  «д» работы и услуги по проектированию в защищенном исполнении:  средств и систем информатизации;  помещений со средствами (системами) информатизации, подлежащими защите;  защищаемых помещений;  «е» (услуги по установке, монтажу, наладке, испытаниям, ремонту средств защиты информации (программных (программно-технических) средств защиты информации)).  Должна быть предоставлена копия лицензии.  Исполнитель должен иметь статус авторизованного партнера Positive Technologies с упоминанием на официальном сайте Positive Technologies. Должна быть предоставлена ссылка, партнерский сертификат и скриншот с веб-сайта.  Исполнитель должен иметь в штате или привлечь к исполнению услуг по договору ГПХ не менее 1 компетентного специалиста, имеющего сертификат Certified Specialist по Positive Technologies Application Firewall от производителя Positive Technologies. Должна быть предоставлена копия сертификата, копия трудового договора/выписка | |  |