Тендерная документация

по тендеру

Внедрение системы Web Application Firewall

в ОАО «Банк Эсхата»

1. Описание общих сведений о предмете тендера

Заказчик:	ОАО «Банк Эсхата»
Общая информация о банке	ОАО «Банк Эсхата» — один из крупнейших участников рынка банковских услуг Таджикистана, осуществляющий все основные виды банковских операций.
Предмет Тендера	Привлечение компаний для поставки и внедрения системы Web Application Firewall
Срок и условия договора	Разовая сделка на сумму/количество или Аккредитация компании как поставщика сроком на 1 год
Способ проведения тендера	открытый
Условия поставки	Склад Заказчика (г.Худжанд).
Дата объявления Тендера	30.08.2024
Дата окончания подачи предложений	30.09.2024
Дата подведения итогов Тендера	При получении недостаточного количества заявок, или в случае несоответствия заявок участников Тендера требованиям Банка, Банк имеет право продлить срок Тендера, соответственно будут продлены сроки подведения итогов Тендера
Место проведения Тендера	Республика Таджикистан, г. Худжанд, ул. Гагарина 135
Место приема заявок	Заявки на участие в Тендере, будут приниматься по электронной почте Секретарем Тендерного Комитета ОАО «Банк Эсхата», телефон: +992 (44) 600 0 600, адрес электронной почты: tender@eskhata.com или почтовым сообщением по адресу: Республика Таджикистан, г. Худжанд, ул. Гагарина 135
Контактное лицо для получения разъяснений	Турсунов Ш.М., нач. отдела ИБ, +992927809352, sh.tursunov@eskhata.com

2. Порядок подачи заявок для участия в Тендере

Заявка на участие в Тендере и необходимые документы должны быть предоставлены в запечатанном конверте с подписью или в электронном формате зашифрованным паролем, с последующим предоставлением пароля от файлов отдельным электронным письмом.

Список требуемых документов:

1. Тендерная заявка (Приложение №1)
2. Коммерческое предложение (Приложение №2)
3. Сведения об участнике тендера, например, в виде презентации
4. Перечень организаций, с которыми участник заключал подобные тендерные договора (опыт работы с другими организациями)
5. Заверенная копия Устава (для юридических лиц)
6. Копия свидетельства или патента на предпринимательскую деятельность (для ИП)
7. Копии лицензий, сертификатов, дилерских полномочий, при наличии
8. Актуальная выписка из единого государственного реестра регистрации юридических лиц и индивидуальных предпринимателей
9. ИНН
10. Финансовые отчеты за последний год с отметкой налогового органа

11. Документы, подтверждающие полномочия представителя на совершение Сделки, а также иные документы, необходимые для идентификации представителя (паспорт и другие документы)

3. Требования к участникам Тендера

К участию в Тендере приглашаются все юридические лица, которые должны соответствовать требованиям, предъявляемым в соответствии с законодательством Республики Таджикистан, в том числе:

1. Обладать правами на объекты интеллектуальной деятельности и иное имущество, являющееся предметом заключаемого договора и подлежащее передаче банку
2. Обладать необходимыми сертификатами, лицензиями или свидетельствами о производстве работ и являющихся предметом заключаемого договора
3. Опыт работы на рынке не менее 1 года и не находиться в процессе реорганизации, ликвидации, или банкротства
4. Обладать профессиональной компетентностью, финансовыми и трудовыми (кадровыми) ресурсами, надежностью, опытом и репутацией, необходимыми для исполнения договора

4. Требования к коммерческому предложению

1. Предложение подается в формате официальных документов организации потенциального поставщика
2. Коммерческое предложение должно быть подписано руководителем организации, имеющим право подписания договорных документов.

5. Техническое требование к предмету тендера/Техническое задание

Техническая задания к предмету тендера приведена в приложение №3.

Приложение №1 к Тендерной документации

Бланк поставщика

(Наименование, адрес, телефон, факс)

Председателю Правления

ОАО «Банк Эсхата»

Дата _____

ТЕНДЕРНАЯ ЗАЯВКА

для участия в тендере на поставку/оказание услуги _____

_____*(название участника тендера)*_____ предлагает осуществить поставку следующей продукции/оказание услуги для ОАО «Банк Эсхата» (далее Банк) _____.

Стоимость_____***(цифрами и прописью)***_____**сомони, в том числе НДС** _____**.**

Неотъемлемой частью настоящей Тендерной заявки является Коммерческое предложение **(Приложение №___).**

К заявке также прилагаются следующие документы:

1._____

2._____

и т.д. (необходимо перечислить все представляемые документы с указанием количества листов и экземпляров).

Мы обязуемся представлять любую информацию, которую Вы сочтете необходимой для проверки сведений, содержащихся в данной Тендерной заявке, или относящихся к нашему опыту или квалификации.

Нам известно, что Банк оставляет за собой право принять или отклонить предложение по данному Тендеру, отменить процесс приобретения и отклонить все предложения в любое время до заключения договора (контракта). Следовательно, Банк не несёт ответственность перед участниками и не принимает на себя обязательство об информировании участников о причинах того или иного действия Банка.

_____ _____ _____

(должность) **(подпись, печать)** **(Ф.И.О.)**

Приложение № 2 к Тендерной документации

Коммерческое предложение
на поставляемую продукцию (оказание услуг)

_____
(наименование участника)

Цены указываются с учетом НДС

№		
1	Наименование оборудования/услуги	
2	Модель (если есть необходимость)	
3	Количество	
4	Цена за одну единицу	
5	Условия оплаты (30%)	
6	Сумма	
7	Срок поставки	
8	Срок гарантии/условия гарантии	
9	Регион доставки	

_____ _____ _____
(должность) **(подпись, печать)** **(Ф.И.О.)**

Приложение № 3 к Тендерной документации

Техническое задание

Система защиты веб-приложений

Содержание

1. Требования к системе

1.1 Требования к назначению Системы

1.1.1 Система должна обеспечивать защиту информационных ресурсов Банка путем выявления инцидентов информационной безопасности, связанных с эксплуатацией уязвимостей веб-приложений, и реагирования на них.

1.1.2 В рамках выполнения своей основной функции Система должна обеспечивать:

- обнаружение и предотвращение атак, направленных на снижение доступности веб-приложений;
- обнаружение и предотвращение атак, направленных на нарушение целостности и доступности обрабатываемой в веб-приложении информации;
- предотвращение утечки конфиденциальной информации через веб-приложения;
- предотвращение несанкционированных изменений внешнего вида и содержимого веб-приложений;
- повышение безопасности веб-приложения в рамках процесса безопасной разработки приложений путем обнаружения и исправления уязвимостей

1.2 Требования к показателям назначения

1.2.1 Должна обеспечиваться обработка веб-трафика с пропускной способностью Системы не менее 300 Мбит/с.

1.2.2 Система должна выдерживать нагрузку до 5000 запросов в секунду (RPS).

2. Требования к функциям (задачам), выполняемым Системой

2.1 Общие требования к функциям (задачам), выполняемым Системой

2.1.1 Система должна поддерживать следующие функции:

- функции анализа и обработки данных;
- функции реагирования;
- функции передачи данных;
- функции хранения данных;
- функции управления;
- функции обновления.

2.2 Требования к функциям анализа и обработки данных (статический анализ файлов)

2.2.1 Система должна поддерживать использование нескольких типов сервисов обработки трафика:

- базовый узел (с ролью обработки трафика);
- узел обработки трафика (управляемый узел);
- внешний агент.

2.2.2 Должны поддерживаться следующие способы обработки трафика:

- в режиме обратного прокси-сервера (reverse proxy) — соединение в разрыв, в котором СЗВП выступает в качестве прокси-сервера между клиентом и защищаемым веб-приложением (в том числе с помощью внешних агентов, расположенных в ИТ-инфраструктуре).

2.2.3 Должны поддерживаться различные варианты установки агентов в ИТ-инфраструктуре Банка:

- в качестве модуля для веб-сервера Nginx;
- в качестве sidecar-контейнера в кластере Kubernetes;
- с интеграцией в Ingress controller в кластере Kubernetes.

2.2.4 Должно поддерживаться определение IP-адреса отправителя веб-трафика (включая случаи с наличием балансировщиков и прокси-серверов).

2.2.5 Должна поддерживаться возможность задания перечня защищаемых серверов, на которых расположены веб-приложения.

2.2.6 Должна поддерживаться возможность создания профилей собираемого (обрабатываемого) трафика веб-приложений, с возможностью указания:

- IP-адресов и портов, которые Система будет использовать для приема клиентских запросов и проксирования их на защищаемое веб-приложение;
- протокола клиентских запросов к серверу;
- серверов из перечня защищаемых серверов веб-приложений;
- режима работы серверов веб-приложений (активный/запасной);
- характера распределения (балансировки) нагрузки между защищаемыми серверами;
- времени ожидания неактивного соединения.

2.2.7 Должны поддерживаться анализ и обработка трафика веб-приложений, передаваемого по протоколам:

- HTTP 1.0, 1.1 и HTTPS, включая TLS 1.0, 1.1, 1.2 и 1.3;
- WebSocket (ws, wss);
- XML-based protocols.

В веб-трафике также должен выполняться анализ данных в нотации:

- XML;
- JSON;
- GraphQL.

2.2.8 Должна обеспечиваться возможность обработки трафика на основании списков IP-адресов в формате CIDR (далее также — глобальных списков); в том числе должны поддерживаться статические и динамические белые и черные списки, устанавливаемые на основе правила:

- для конкретного приложения;
- для всех приложений.

2.2.9 Должна обеспечиваться возможность переключения между режимами защиты (без мер защиты, обнаружение и изменение содержимого, все меры защиты).

2.3 Требования к функциям реагирования

2.3.1 Должны поддерживаться наборы правил обработки трафика, настроенные на защиту объектов (ресурсов) на базе технологий, указанных в названии набора правил:

- Apache Struts — включает только те правила, которые предназначены для защиты веб-приложений, разработанных на фреймворке Apache Struts;
- ASP.NET — включает только те правила, которые предназначены для защиты веб-приложений, созданных на платформе ASP.NET;
- Java — включает только те правила, которые предназначены для защиты веб-приложений, разработанных на языке Java;
- Joomla CMS — включает только те правила, которые предназначены для защиты веб-приложений, основанных на системе управления контентом Joomla;
- LAMP (PHP, Apache, MySQL) — включает только те правила, которые предназначены для защиты веб-приложений, разработанных при помощи инструментов PHP, Apache или MySQL;
- Exchange — включает только те правила, которые предназначены для защиты почтового сервера;
- Node.js — включает только те правила, которые предназначены для защиты веб-приложений, созданных на платформе Node.js;
- PHP — включает только те правила, которые предназначены для защиты веб-приложений, разработанных на языке PHP;
- Default template (стандартный шаблон) — включает правила всех остальных системных наборов.

2.3.2 Для системных правил должны быть указаны:

- наименование правила;
- статус активности правила (включено или отключено);
- принадлежность к системному набор правил;
- действие при срабатывании;
- принадлежность к группе правил;
- точность определения атаки правилом (по оценке экспертов);
- фаза срабатывания правила (запрос/ответ);
- метки (теги), помогающие при сортировке;
- классификация правила (CAPEC, WASC, OWASP) с указанием года (при наличии);
- тип угрозы безопасности, обнаруживаемой в результате срабатывания правила;
- уровень опасности события безопасности, зарегистрированного в результате срабатывания правила.

2.3.3 Должна поддерживаться возможность создания новых пользовательских правил (набора пользовательских правил), в том числе должны поддерживаться возможности задания:

- наименования правила;
- описания (опционально);
- меток (тегов), помогающих при сортировке;
- классификации правила (CAPEC, WASC, OWASP) с указанием года (опционально);
- типа события (атака, уязвимость, инцидент, информация);
- уровня опасности события, регистрируемого в результате срабатывания пользовательского правила (низкий, средний, высокий, критический);
- конфигурации правила (включая возможность задания пользовательских параметров и привязку к конкретному параметру, например списку IP-адресов в формате CIDR, зарегистрированному в системе);
- действий при срабатывании.

2.3.4 Должна поддерживаться возможность группировки системных правил на основе:

- типа события безопасности;
- точности;
- фазы срабатывания правила;
- уровня опасности;
- предустановленной группы правил.

2.3.5 Должна поддерживаться группировка предустановленных правил по решаемой задаче, вектору атаки или технологии (там, где это применимо к набору правил):

- контроль доступа;
- боты;
- политики браузера;
- CSRF;
- XSS;
- эксплуатация уязвимостей из списка CVE;
- загрузка файлов;
- нарушение структуры HTTP;
- ImageMagick;
- внедрение;
- репутация IP-адреса;
- J2EE;
- безопасность JWT;
- предварительная обработка;
- доступность важных файлов;

- SSRF;
- сессии;
- внедрение SQL-кода;
- исполнение вредоносных файлов;
- безопасность XML.

2.3.6 Должна поддерживаться возможность группировки пользовательских правил на основе:

- типа события безопасности;
- фазы срабатывания правила;
- уровня опасности.

2.3.7 Должны поддерживаться стандартные действия для правил, применяемые по выбору пользователя:

- block (отправить пользователю страницу, которая будет отображаться при блокировании запросов вместо ответа защищаемого сервера);
- log to db (записать информации об обнаруженных событиях безопасности в базу данных Системы);
- send to syslog server;
- skip rules (только для статических ресурсов).

2.3.8 Должна поддерживаться возможность создания пользовательских действий для правил на основе типа этих действий:

- log to db;
- send custom response;
- send to syslog server.

2.3.9 Должна поддерживаться возможность редактирования пользовательских правил.

2.3.10 Должна поддерживаться возможность создания исключений для правил.

2.3.11 Должна поддерживаться возможность создания шаблонов политик безопасности на базе существующих правил (системных и пользовательских). Настройка политик безопасности должна поддерживаться как для отдельных приложений, так и для нескольких приложений одновременно.

2.3.12 Должна поддерживаться возможность отключения конкретных правил в существующих шаблонах политик безопасности (т. е. редактирование шаблонов).

2.3.13 Должна обеспечиваться возможность применения глобальных списков в качестве параметров правил и шаблонов политик безопасности.

2.3.14 Должна поддерживаться возможность удаления пользовательских шаблонов политик безопасности.

2.3.15 Должны обеспечиваться обнаружение признаков атак на веб-приложения и регистрация событий безопасности на основе установленных правил обработки трафика (защиты веб-приложения).

2.3.16 Должна поддерживаться агрегация единичных событий безопасности, зарегистрированных одним правилом для одного IP-адреса в рамках веб-приложения. Результаты агрегации должны регистрироваться в виде «событий агрегации».

2.3.17 Должна сохраняться следующая информация о событиях агрегации:

- дата возникновения первого вошедшего в событие агрегации события безопасности;
- дата возникновения последнего вошедшего в событие агрегации события безопасности;
- название правила, срабатывания которого привели к созданию события агрегации;
- количество срабатываний правила, вошедших в событие агрегации;
- время, за которое фактически было собрано событие агрегации;
- IP-адрес отправителя запросов, вызвавших срабатывания правила и сборку события агрегации;

- дата, до которой IP-адрес отправителя будет находиться в черном списке;
- правило, осуществляющее фактическую блокировку адресов, находящихся в списке заблокированных;
- название веб-приложения, для которого создано событие агрегации.

2.3.18 Должна поддерживаться:
- сортировка событий по любому из отображаемых атрибутов события;
- фильтрация событий по любому из отображаемых атрибутов.

2.3.19 Должна поддерживаться возможность дополнения глобального списка IP-адресов на основе возникновения событий агрегации.

2.3.20 Должна обеспечиваться возможность отслеживания попыток доступа пользователя к ресурсам защищаемого веб-приложения, осуществляемых на основании применяемых методов аутентификации с использованием:
- аутентификации через веб-форму;
- базовой аутентификации.

В том числе должны фиксироваться все успешные и неуспешные попытки аутентификации пользователя.

2.3.21 Должны обнаруживаться попытки доступа к интерфейсу администрирования Apache Tomcat Manager с использованием пар «логин — пароль», указанных в списке запрещенных значений.

2.3.22 Должна поддерживаться возможность обновления (дополнения) списка запрещенных значений пар «логин — пароль».

2.3.23 Должно поддерживаться обнаружение использования ботов для автоматического сканирования или получения данных сайта (на основе заголовка User-Agent).

2.3.24 Должна поддерживаться возможность обновления (дополнения) списка обнаруживаемых заголовков User-Agent.

2.3.25 Должна поддерживаться возможность обнаружения автоматизированной активности путем добавления сервиса защиты reCAPTCHA v3 на страницу защищаемого веб-приложения.

2.3.26 Должна поддерживаться возможность обнаружения и контроля автоматизированной активности путем ограничения количества HTTP-запросов от одного клиента за установленный период времени. Должны поддерживаться следующие параметры:
- маршруты;
- скорость.

2.3.27 Должно обеспечиваться выявление сканирования на уязвимости.

2.3.28 Должно обеспечиваться выявление сканирования сервера Apache Tomcat запросами на наличие доступа к стандартным путям с примерами Java-сервлетов и JSP-страниц, которые по умолчанию устанавливаются вместе с Apache Tomcat в версиях 4.x–7.x.

2.3.29 Должно обеспечиваться обнаружение попыток перебора путей к административному интерфейсу сервера Apache Tomcat на основе справочника стандартных путей.

2.3.30 Должна поддерживаться возможность дополнения справочника стандартных путей.

2.3.31 Должна поддерживаться возможность модификации ответов от защищаемого веб-приложения путем добавления или замены заголовков:
- Referrer-Policy, настраивающего уровень детализации для включения в заголовок Referrer при уходе со страницы;
- X-Content-Type-Options, запрещающего браузерам выполнение контента, для которого не установлен правильный MIME-тип данных;
- X-Frame-Options, запрещающего браузеру загружать страницу во Frame/Iframe;
- X-XSS-Protection для включения фильтрации XSS.

2.3.32 Должна поддерживаться возможность задания режима принудительного использования протокола HTTPS веб-приложением путем задания заголовка Strict-Transport-Security с возможностью установки срока работы режима.

2.3.33 Должна поддерживаться возможность модификации ответов куки (cookie) путем принудительной установки атрибутов безопасности:

- httpOnly;
- secure;
- sameSite.

2.3.34 Должны обнаруживаться и блокироваться CSRF-атаки путем проверки заголовков Origin и Referer на наличие запрещенных значений URL.

2.3.35 Должно поддерживаться обнаружение и блокирование межсайтового выполнения сценариев (XSS), в том числе:

- XSS в контексте HTML;
- XSS в контексте JavaScript;
- XSS в контексте URL;
- отраженное XSS в контексте HTML.

2.3.36 Должны поддерживаться правила, направленные на контроль эксплуатации уязвимостей из списка CVE.

2.3.37 Должны поддерживаться следующие правила из группы правил «загрузка файлов»:

- проверка MIME-типа файла из тела запроса на соответствие списку разрешенных типов;
- проверка на наличие запрещенных расширений файлов;
- проверка файла на наличие вредоносного HLS-плейлиста в файлах типа AVI и M3U;
- проверка на наличие вредоносного веб-шелла;
- проверка на наличие уязвимости Zip Slip;
- проверка PHP-архива на наличие PHAR-эксплойта.

2.3.38 Должна поддерживаться возможность добавления MIME-типов в список запрещенных.

2.3.39 Должна поддерживаться возможность добавления расширений в список запрещенных.

2.3.40 Должны поддерживаться правила, направленные на контроль структуры HTTP-запроса к защищаемому веб-серверу:

- проверка на наличие одинаковых заголовков в запросе;
- проверка наличия тела запроса у запросов GET и HEAD;
- проверка наличия запрещенных методов в HTTP-запросе;
- проверка версии HTTP-запроса;
- проверка наличия заголовка Content-Length или Transfer-encoding в POST-запросе;
- проверка корректности значения заголовка Content-Length (Transfer Encoding);
- проверка допустимости значения заголовка Content-Type в запросе;
- проверка соответствия значения заголовка Accept-Encoding к списку разрешенных значений;
- проверка наличия заголовка Host в запросе по протоколу HTTP/1.1;
- проверка кодировок в HTTP-запросе.

2.3.41 Должно поддерживаться обнаружение и блокирование атак, направленных на уязвимости набора программ для чтения и редактирования файлов графических форматов ImageMagick, в том числе атак направленных на:

- удаленное выполнение команд с помощью библиотеки Ghostscript (с возможностью добавления частей HTTP-запроса в исключения или приоритеты проверки);

- попытки эксплуатации уязвимости ImageTragick;
- кражу данных с помощью GIF-файлов в ImageMagick версии 7.0.6-1 и GraphicsMagick версии 1.3.26;
- кражу данных с помощью XBM-файла при обработке таких файлов с помощью ImageMagick версий 7.0.8–9.

2.3.42 Должны поддерживаться механизмы защиты от следующих атак, направленных на внедрение небезопасного кода:

- некорректно сформированный JSON- или XML-код в теле запроса;
- внедрение CSS-кода;
- внедрение кода Expression Language;
- расщепление HTTP-ответов;
- небезопасная десериализация объектов Java;
- внедрение в LDAP-запросы;
- внедрение локальных файлов (LFI);
- внедрение в Memcached;
- внедрение NoSQL-кода;
- открытое перенаправление (Open Redirect);
- наличие результата выполнения команды id в ответе;
- внедрение команд ОС;
- выход за пределы каталога;
- внедрение объектов PHP;
- удаленное выполнение кода (RCE), связанное с десериализацией параметров;
- удаленное выполнение кода (RCE) в Ruby, связанное с десериализацией и цепочкой гаджетов;
- внедрение во включения на стороне сервера (SSI);
- внедрение JavaScript-кода на стороне сервера (SSJI);
- внедрение в серверный шаблон (SSTI);
- внедрение XPath-кода;
- внедрение XSLT на стороне сервера;
- внедрение объектов YAML.

2.3.43 Должны поддерживаться следующие правила из группы правил «Репутация IP-адреса»:

- блокирование клиентов по IP-адресу из диапазона адресов национального или регионального провайдера (на базе GeoIP2);
- блокирования клиентов по IP-адресу из глобального (статического списка);
- блокирования клиентов по IP-адресу из глобального (динамического списка).

2.3.44 Должны обнаруживаться и блокироваться атаки, направленные на уязвимости Java 2 Enterprise Edition, в том числе:

- атака на уязвимость во фреймворке Apache Wicket, которая приводит к утечке конфигурационных и программных файлов (таких как .sf, .tld, .class, .xml и .jar) из каталогов META-INF и WEB-INF;
- атака на веб-приложения, разработанные на фреймворке Grails, направленная на получение доступа к ресурсам, расположенным в каталогах /WEB-INF и /META-INF;
- атака через утечку данных на сервере Jetty версии ниже 9.2.9.v20150224;
- атака через удаленное выполнение кода (RCE) с помощью Spring Boot.

2.3.45 Должны поддерживаться следующие правила проверки JSON Web Token (JWT):

- проверка значения заголовка alg на значение none;
- проверка подмены открытого ключа JWT.

2.3.46 Должна поддерживаться проверка ответов приложения на наличие признаков выполнения вредоносного сценария (веб-шелла).

2.3.47 При проведении обработки передаваемых данных должны выполняться следующие предварительные проверки и действия с трафиком:

- декодирование параметров HTTP-трафика;
- проверка HTTP-запросов с типом содержимого multipart/form-data на соответствие;
- проверка статических ресурсов (с возможностью задания перечня исключений из проверки);
- нормализация параметров PHP (GET-, POST-, куки);
- нормализация параметров ASP.NET;
- проверка превышения ограничений для JSON (с возможностью задания перечня ограничений атрибутов JSON);
- проверка превышения ограничений для GraphQL (с возможностью задания перечня ограничений атрибутов GraphQL);
- проверка превышения ограничения для протокола HTTP (с возможностью задания перечня ограничений атрибутов HTTP-запросов, куки, заголовков, других частей);
- проверка превышения ограничений для XML (с возможностью задания перечня ограничений атрибутов XML-документа).

2.3.48 Должно поддерживаться рекурсивное декодирование параметров в запросах с возможностью задания глубины рекурсии.

2.3.49 Должны обнаруживаться и блокироваться случаи компрометации сессии пользователя, а именно:
- использование сессионного идентификатора пользователя с разных IP-адресов;
- разглашение информации о сессии через параметры URL.

2.3.50 Должны поддерживаться обнаружение и блокирование атак типа «внедрение SQL-кода» (SQL-injection):
- на основе ошибок сервера;
- на основе времени;
- на основе параметров запроса.

2.3.51 Должна поддерживаться возможность обнаружения и блокирования атак типа «подмена запросов на стороне сервера» (server-side request forgery, SSRF,).

2.3.52 Должно обеспечиваться обнаружение и блокирование атак на уязвимости при обработке документов XML путем проверки:
- наличия обращений к внешним сущностям (XML external entities, XXE) в XML_документе;
- использования определения типа документа (document type definition, DTD) из внешнего файла для XML-документа.

2.4 Требования к функциям передачи данных

2.4.1 Должны предоставляться программные интерфейсы (REST API) для автоматизации задач по управлению системой с помощью внешних программных средств.

2.4.2 Должна обеспечиваться возможность получения данных об очередях на дисках собственных узлов системы.

2.5 Требования к функциям хранения данных

2.5.1 Должно обеспечиваться хранение данных системы на базовых узлах, в том числе:
- событий безопасности;
- параметров безопасности и данных о конфигурации системы;
- крупных бинарных объектов, таких как резервные копии и отчеты.

2.6 Требования к функциям управления

2.6.1 Должна быть обеспечена мультиарендность, позволяющая пользователям работать в изолированном пространстве защищаемых приложений, связанных с ними событий безопасности и политик безопасности.

2.6.2 Должна обеспечиваться возможность управления собственными узлами Системы через консольный интерфейс (SSH) — для выполнения системных настроек.

2.6.3 Должна обеспечиваться возможность управления функциями Системы через веб-интерфейс (HTTPS).

2.6.4 Возможность управления Системой через любой из интерфейсов должна предоставляться только авторизованным (уполномоченным) пользователям.

2.6.5 Должна обеспечиваться реализация ролевой модели управления доступом к функциям Системы, доступным через веб-интерфейс. В том числе должны обеспечиваться:

- создание, редактирование и удаления пользовательских ролей;
- управление разрешениями, назначаемыми каждой роли.

2.6.6 Должна обеспечиваться возможность управления (в том числе создание, изменение, удаление, блокировка) учетными записями пользователей Системы:

- логинами и паролями;
- ролями (только веб-интерфейс).

2.6.7 Должна обеспечиваться регистрация событий, связанных с действиями пользователей системы и системными операциями.

2.6.8 Должна обеспечиваться возможность создания изолированных пространств:

- для собственных узлов;
- для агентов.

2.6.9 Должна обеспечиваться возможность загрузки ключей для расшифровки HTTPS-трафика, отправляемого на защищаемые серверы.

2.6.10 Должна обеспечиваться возможность загрузки цепочки SSL-сертификатов для расшифровки HTTPS-трафика, отправляемого на защищаемые серверы.

2.6.11 Должна обеспечиваться визуализация данных о событиях безопасности в виде таблиц и гистограмм на ленте событий.

2.6.12 Должна обеспечиваться возможность указания временного периода, за который отображаются события безопасности, зафиксированные Системой.

2.6.13 Должна обеспечиваться возможность обновления данных о событиях безопасности в автоматическом и «ручном» режимах.

2.6.14 Должна обеспечиваться возможность отправки записей обращений (access.log) к защищаемому веб-приложению в систему регистрации событий и выявления инцидентов информационной безопасности (SIEM).

2.6.15 Должна поддерживаться возможность генерации отчетов о работе системы, доступных к выгрузке из графического интерфейса. Выгрузка отчетов должна осуществляться в формате PDF.

2.6.16 Должна обеспечиваться возможность создания резервных копий Системы, содержащих сведения о конфигурации системы, в том числе:

- параметры контроля доступа;
- параметры безопасности.

2.6.17 Должен поддерживаться экспорт глобальных списков.

2.6.18 Должен обеспечиваться мониторинг состояния Системы и предоставление в веб-интерфейсе следующих данных о состоянии Системы:

- общее состояние системы;
- состояние узлов кластера;
- состояние сервисов;
- загрузка ЦПУ;
- объем используемой памяти;
- нагрузка на базу данных событий безопасности;
- нагрузка на базу данных конфигурации;
- средняя загрузка системы;
- пропускная способность.

2.6.19 Должно обеспечиваться отслеживание статуса применения конфигурации.

2.7 Требования к функциям обновления

2.7.1 Должно обеспечиваться автоматизированное обновление баз знаний (правил защиты).

3. Технологические требования

3.1 Требования к архитектуре системы

3.1.1 Система должна представлять собой локальное решение, разворачиваемое внутри защищаемого периметра.

3.1.2 Система должна быть построена на основе программного и аппаратного обеспечения, размещаемого на объектах Банка с учетом возможной территориальной распределённых площадок.

3.1.3 Система должна поддерживать одно серверные и много серверные конфигурации.

3.1.4 Система должна поддерживать возможность работы в режиме отказоустойчивого кластера.

3.1.5 Система должна поддерживать конфигурации с использованием как внешних, так и внутренних балансировщиков нагрузки.

3.1.6 Система должна поддерживать возможность подключения внешних агентов или дополнительных серверов обработки трафика.

3.1.7 Требования к техническому обеспечению Системы должны быть определены (уточнены) на стадии технического проектирования Систем. В том числе определяются:

- перечень и характеристики программного и аппаратного обеспечения, необходимого для выполнения Системой собственных функций;
- необходимость использования конкретной конфигурации;
- необходимость работы в режиме отказоустойчивого кластера;
- необходимость работы с использованием конкретных балансировщиков;
- необходимость использования внешних агентов или дополнительных серверов обработки трафика.

3.2 Требования по интеграции с другими системами

3.2.1 Система должна обеспечивать возможность интеграции со следующими смежными системами:

- системой регистрации событий и выявления инцидентов информационной безопасности (системой класс SIEM) — для передачи сведений об обнаруженных угрозах;
- внешними системами автоматизации;
- системой точного времени NTP Банка — для обеспечения единых меток даты/времени;
- DNS-серверами.

4. Требования к технической поддержке

4.1. Исполнитель должен обеспечить консультационную и техническую поддержку Системы в соответствии со следующими требованиями:

- наличие выделенной линии службы приема и разрешения технических запросов по e-mail и телефону;
- режим оказания технической поддержки Исполнителя: с понедельника по пятницу в рабочее время Банка.
- максимальное время реакции техподдержки для заявок: критичного приоритета – в течение 2 (Двух) часов, высокого приоритета – в течение 4 (Четырёх) часов, среднего приоритета – в течение 6 (Шести) часов, низкого приоритета – в течение 8 (Восьми) часов.

4.2. Исполнитель должен обеспечить предоставление услуг в рамках технической поддержки, в том числе:

- возможность получения консультаций специалистов по техническим вопросам, связанным с настройкой, эксплуатацией, конфигурированием, управлением исправным ПО, в течение времени обслуживания;
- восстановление работоспособности ПО в режиме обслуживания;
- Диагностика состояния ПО при получении заявки от Лицензиата о неисправности, поиск и локализацию неисправностей ПО;
- ответы на сообщения об ошибках в ПО и определение того, является ли данная ошибка результатом сбоя самого ПО или же она вызвана проблемами, связанными с внешними условиями существования или установкой ПО. Лицензиат обязан предоставить Лицензиару информацию, достаточную для того, чтобы воспроизвести данную ошибку на основной копии ПО, и включающую в себя подробное описание проблемы, регистрационные файлы, дампы оперативной памяти, файлы данных и т.п.
- предоставление Лицензиату возможности бесплатно скачивать обновления ПО, новые версии и релизы в течение срока сопровождения, получать лицензионный ключ для их установки;
- Пере активация (повторная активация) ПО, при необходимости;
- предоставление актуальной документации по настройке и эксплуатации ПО.

4.3. SLA

Таблица 1. Уровень критичности функционирования системы

Критический приоритет	Высокий приоритет	Средний приоритет	Низкий приоритет
Ошибка, приводящая к устойчивым сбоям в функционировании технических средств Системы, полностью нарушающим работоспособность Системы, включая полную или частичную остановку, перманентную перезагрузку Системы, потерю или нарушение целостности данных, влекущую за собой существенную деградацию производительности Системы и СУБД.	Ошибка, приводящая к неустойчивым сбоям в функционировании технических средств Системы частично нарушающим работоспособность Системы, включая потерю части функциональности, потерю части данных или их целостности, заметное снижение производительности Системы и др. Проблемы, связанные с неработоспособностью отдельных узлов Системы, напрямую не затрагивающих процессы сбора, анализа и журналирования сетевого трафика.	Ошибка, приводящая к отдельным (разовым) сбоям в функционировании технических средств Системы. Ошибка, связанная с нарушением работоспособности технических средств отдельных АРМ.	Система работает в нормальном режиме. Запросы потенциального функционала, запрос на разработку и внедрение дополнительных услуг и функций в существующую Систему, иные консультационные запросы Банка.

Таблица 2. Реагирование

Время реакции на запрос (в зависимости от приоритета) С Понедельника до Пятницу.	Критический	до 1 часа
	Высокий	4 часа
	Средний	6 рабочих часов
	Низкий	8 рабочих часов

5. Требования к услугам по внедрению Системы

4.4. Работы должны включать следующие мероприятия:

- инсталляция системы в информационной инфраструктуре Банка;
- настройка стандартных и необходимых правил для 3-х Web приложений Банка;
- интеграция с SIEM системой Банка;
- обучение специалистов Банка по работе с системой, включая формирования новых правил.

4.5. Срок и задачи по внедрению должны согласоваться с Банком;

4.6. Заранее согласовать список необходимых ресурсов для внедрения с Банком;

4.7. В ходе оказания Услуг не должна быть нарушена работоспособность информационных систем Банка и не должна быть повреждена информация, хранящаяся или обрабатываемая в них.