|  |
| --- |
| У Т В Е Р Ж Д А Ю |
| Директор Дирекции по инфраструктуре и информационной безопасности ПАО «НЛМК» |
| Медвенский Л.И. |
| «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2024 г. |

|  |
| --- |
| **ФУНКЦИОНАЛЬНО-ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ** |
| Передача прав использования программного обеспечения,  оказание услуг внедрения и технической поддержки  Системы защиты web-приложений (WAF) |

|  |  |
| --- | --- |
| **Заказчик:** | Публичное акционерное общество «Новолипецкий металлургический комбинат» |
| **Проект:** | "РПИБ-2 система защиты web-приложений (WAF)" |
| **Версия:** | 0.1 |

|  |  |
| --- | --- |
| **Страниц:** | 51 |

**ОГЛАВЛЕНИЕ**

[ТЕРМИНЫ И СОКРАЩЕНИЯ 4](#_Toc178243441)

[1. ОБЩИЕ СВЕДЕНИЯ 5](#_Toc178243442)

[1.1. Нормативно-методические документы (НМД) 5](#_Toc178243443)

[2. ОПИСАНИЕ БИЗНЕС-КЕЙСА 6](#_Toc178243444)

[3. ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ К СИСТЕМЕ 6](#_Toc178243445)

[3.1. Ключевые группы функций и функции, реализуемые системой 7](#_Toc178243446)

[3.2. Требования к функциям, выполняемым системой 7](#_Toc178243447)

[3.3. Функционально-ролевая модель 16](#_Toc178243448)

[3.4. Требования к методологической проработке 17](#_Toc178243449)

[3.4.1. Общие требования к интеграции с существующими системами 17](#_Toc178243450)

[3.4.2. Требования к взаимодействию со смежными системам 17](#_Toc178243451)

[3.4.3. Требования к доработке в интегрируемых системах 18](#_Toc178243452)

[3.5. Требования к архитектуре системы 18](#_Toc178243453)

[3.5.1. Требование к проектированию архитектуры 18](#_Toc178243454)

[4. НЕФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ К СИСТЕМЕ 19](#_Toc178243455)

[4.1. Требования к расширяемости и масштабируемости 19](#_Toc178243456)

[4.2. Требования к надежности системы 19](#_Toc178243457)

[4.3. Требования к мониторингу системы 20](#_Toc178243458)

[4.3.1. Мониторинг инфраструктуры 20](#_Toc178243459)

[4.4. Требования к производительности 20](#_Toc178243460)

[4.5. Требование к лингвистическому обеспечению 21](#_Toc178243461)

[4.6. Требования к технологическому стеку 21](#_Toc178243462)

[4.7. Требования к комплекту поставки 22](#_Toc178243463)

[4.8. Требования к структуре команды 22](#_Toc178243464)

[5. ТРЕБОВАНИЯ К ИТ-ИНФРАСТРУКТУРЕ 24](#_Toc178243465)

[5.1. Общие требования к системе 24](#_Toc178243466)

[5.2. Требования к размещению 25](#_Toc178243467)

[5.3. Требования к сетевому сегментированию 25](#_Toc178243468)

[5.4. Требования к резервному копированию 26](#_Toc178243469)

[5.4.1. Общие требования 26](#_Toc178243470)

[5.4.2. Прочие компоненты системы 26](#_Toc178243471)

[5.5. Инфраструктурные требования к организационному обеспечению 26](#_Toc178243472)

[5.5.1. Инфраструктурные требования к Проектному решению на систему 26](#_Toc178243473)

[5.5.2. Инфраструктурные требования к проверке производительности 26](#_Toc178243474)

[5.5.3. Требования к проверке состояния здоровья системы 27](#_Toc178243475)

[5.5.4. Требования к плану восстановления системы 27](#_Toc178243476)

[5.6. Класс критичности создаваемой системы 27](#_Toc178243477)

[6. ТРЕБОВАНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ 28](#_Toc178243478)

[6.1. Требования к функциям управления доступом 29](#_Toc178243479)

[6.2. Требования к функциям регистрации и учета 30](#_Toc178243480)

[6.3. Требования к функциям обеспечения целостности 31](#_Toc178243481)

[6.4. Требования к функциям криптографической защиты информации 31](#_Toc178243482)

[6.5. Защита технических средств, систем связи и передачи данных 32](#_Toc178243483)

[6.6. Требования к защите информации от несанкционированного доступа 32](#_Toc178243484)

[6.7. Требования к переводу системы в промышленную эксплуатацию 33](#_Toc178243485)

[7. ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ПУСКО-НАЛАДОЧНЫХ РАБОТ 33](#_Toc178243486)

[8. ТРЕБОВАНИЯ К ПОРЯДКУ КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ 34](#_Toc178243487)

[8.1. Состав и содержание работ 34](#_Toc178243488)

[8.2. Требования к контролю и приемке системы 34](#_Toc178243489)

[8.3. Проведение предварительных испытаний 34](#_Toc178243490)

[8.4. Проведение опытной эксплуатации 35](#_Toc178243491)

[8.5. Требования к поддержке в рамках опытной эксплуатации 35](#_Toc178243492)

[8.6. Проведение приемочных испытаний 35](#_Toc178243493)

[9. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ РАБОТ 35](#_Toc178243494)

[10. ТРЕБОВАНИЯ К ГАРАНТИЙНОМУ ОБСЛУЖИВАНИЮ 36](#_Toc178243495)

[11. ТРЕБОВАНИЯ К ОБУЧЕНИЮ ПЕРСОНАЛА 36](#_Toc178243496)

[12. ТРЕБОВАНИЯ К ИНФОРМИРОВАНИЮ И КОММУНИКАЦИИ 37](#_Toc178243497)

[13. ТРЕБОВАНИЯ К ПАТЕНТНОЙ ЧИСТОТЕ 38](#_Toc178243498)

[14. ТРЕБОВАНИЕ К ТЕХНИЧЕСКОЙ ПОДДЕРЖКЕ 38](#_Toc178243499)

[14.1. Требования к реактивной технической поддержке 38](#_Toc178243500)

[14.2. Требование к проактивной технической поддержке 39](#_Toc178243501)

[14.3. Требование к работам по заявкам 40](#_Toc178243502)

[15. ТРЕБОВАНИЕ К ДОКУМЕНТИРОВАНИЮ 40](#_Toc178243503)

[16. ТРЕБОВАНИЕ К УСЛОВИЯМ ДОГОВОРА 41](#_Toc178243504)

[ЛИСТ СОГЛАСОВАНИЯ 42](#_Toc178243505)

[ПРИЛОЖЕНИЕ А 43](#_Toc178243506)

[ПРИЛОЖЕНИЕ Б 46](#_Toc178243507)

[ПРИЛОЖЕНИЕ В 51](#_Toc178243508)

## ТЕРМИНЫ И СОКРАЩЕНИЯ

Таблица 1 - Термины и сокращения

|  |  |
| --- | --- |
| **Термин** | **Определение** |
| AD | Microsoft Active Directory |
| CAB | Change Advisory Board - комитет по изменениям |
| CIDR | Classless Inter-Domain Routing - бесклассовая адресация, при которой количество адресов в сети определяется исключительно маской подсети |
| CSP | Content Security Policy - стандарт защиты сайтов от атак с внедрением контента |
| CSRF | Cross-Site Request Forgery - межсайтовая подделка запросов; уязвимость, при которой атакующий выполняет несанкционированные действия на сайте от имени авторизованного пользователя |
| CVE | Common Vulnerabilities and Exposures - список наиболее распространенных уязвимостей в программном обеспечения |
| DRP | Disaster recovery plan - план аварийного восстановления |
| IDOR | Insecure direct object references - уязвимость, которая позволяет получить несанкционированный доступ к веб-страницам или файлам |
| JWT | JSON Web Token - открытый стандарт для создания токенов доступа, основанный на формате JSON |
| LDAP | Lightweight Directory Access Protocol - протокол для доступа к каталогу AD |
| SIEM | Security Information and Event Management - система сбора и корреляции событий ИБ |
| SOAR | Security Orchestration, Automation and Response - система оркестрации, автоматизации и реагирования на инциденты ИБ |
| SSRF | Server-Side Request Forgery - поделка запросов со стороны сервера; уязвимость, при которой злоумышленник может отправлять фальшивые запросы с сервера на другие внутренние или внешние ресурсы |
| WAF | Web Application Firewall - система защиты веб-приложений |
| XSS | Cross-Site Scripting - межсайтовый скриптинг; уязвимость, при которой вредоносный код внедряется в страницы веб-приложения |
| АВ | Антивирус |
| БД | База данных |
| ВМ | Виртуальная машина |
| ЗНИ | Запрос на изменение |
| ИБ | Информационная безопасность |
| ИР | Информационный ресурс |
| ИС | Информационная система |
| ИТ | Информационные технологии |
| МБР | Менеджер бизнес решений |
| НЛМК | Новолипецкий металлургический комбинат |
| НМД | Нормативно-методические документы |
| ОС | Операционная система |
| ПАК | Программно-аппаратный комплекс |
| РП | Руководитель проекта |
| ТП | Техническая поддержка |
| УИ | Управление изменениями |
| УИБ | Управление информационной безопасностью |
| УК | Управляющий комитет |
| ФТТ | Функционально-технические требования |
| ЦОД | Центр обработки данных |

## ОБЩИЕ СВЕДЕНИЯ

Настоящие функционально технические требования (далее – ФТТ) определяют функциональные и технические требования к конкурсному выбору, доработке и внедрению системы защиты веб-приложений от несанкционированного доступа (далее - Система), требования интеграции со смежными системами, требования к ИТ-инфраструктуре, требования к информационной безопасности, документации, порядку приемо-сдаточных испытаний.

Информация о предприятиях, затрагиваемых в процессе разработки проекта, представлена в Таблице 2.

Таблица 2 - Границы проекта

|  |  |  |
| --- | --- | --- |
| **№ п.п.** | **Наименование предприятия** | **Адрес объекта** |
| 1. | ПАО «НЛМК»\* | г. Липецк, пл. Металлургов, д.2 |

\*Все площадки группы НЛМК на территории Российской Федерации

## Нормативно-методические документы (НМД)

Внедрение системы должно проводиться с учетом требований следующих нормативно-методических документов:

* Указ Президента Российской Федерации от 01.05.2022 № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации";
* Приказ ФСТЭК России от 18.02.2013 № 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";
* Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утв. приказом ФСТЭК России от 02.06.2020 № 76.

## ОПИСАНИЕ БИЗНЕС-КЕЙСА

**Ключевая проблема:** использование WAF системы от зарубежного вендора (США). Текущая версия системы достигла окончания жизненного цикла. В связи с введенными санкциями отсутствует возможность закупки новой версии, установки обновлений и отсутствует техническая поддержка.

**Проблема для Группы НЛМК:** использование устаревших инструментов защиты веб-приложений от несанкционированного доступа снижает общий уровень защищенности группы НЛМК в области ИБ, увеличивает риск возникновения инцидентов ИБ, что может повлечь к потере контроля за инфраструктурой и репутационным рискам. Одновременно с этим возникают риски возникновения штрафных санкций.

**Проблема для сотрудников управления информационной безопасностью (УИБ):**

* Увеличение рисков информационной безопасности, снижение доступности веб-приложений, риски нарушения конфиденциальности информации.
* Невозможность противостояния современным угрозам ввиду отсутствия своевременного обновления системы.
* Текущий процесс публикации веб-приложений за WAF непрозрачен и не формализован.

**Решение:**

* Заместить текущую WAF систему отечественным аналогом.
* Проработать и формализовать процесс публикации веб-приложений за WAF.

## ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ К СИСТЕМЕ

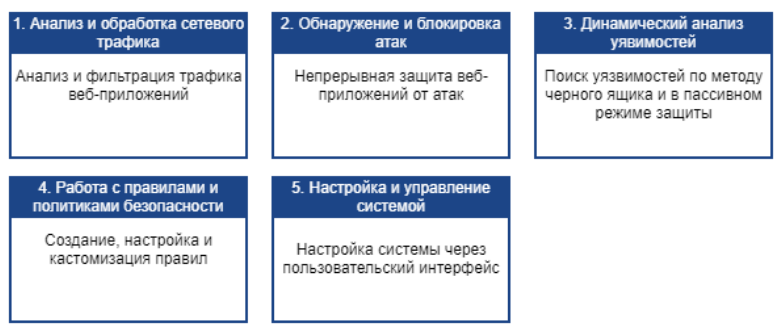
При формировании коммерческого предложения, в случае отсутствия одной или нескольких описанных в разделе 3 функций, участник конкурса обязан:

* подтвердить, что данный функционал будет реализован и внедрен в рамках проекта без увеличения его сроков;
* или
* предложить альтернативную реализацию недостающего функционала;
* произвести расчет стоимости/трудозатрат реализации недостающего функционала;
* произвести оценку сроков реализации и отразить их в коммерческом предложении.

## Ключевые группы функций и функции, реализуемые системой

Функциональные блоки Системы, описаны на рисунке 1.

Рисунок 1 - Функциональные блоки и компоненты системы



## Требования к функциям, выполняемым системой

Система защиты веб-приложений от несанкционированного доступа должна обеспечивать выполнение функций, описанных в таблице 3.

Таблица 3 - Требования к функциям

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **п.** | **Функция** | **п.п.** | **Описание требований к функции** | Приоритет |
| 1 | Анализ и обработка сетевого трафика | 1.1 | Система должна осуществлять контроль сетевого трафика и выполнять фильтрацию (разрешение или блокировку) трафика в соответствии с заданным правилами.  Требования по работе с правилами в Системе описаны в п. 4 таблицы. | Первый |
| 1.2 | Система должна обеспечивать возможность задания перечня защищаемых серверов, на которых расположены веб-приложения. | Первый |
| 1.3 | Система должна обеспечивать возможность создания профилей обрабатываемого трафика веб-приложений. | Первый |
| 1.4 | Система должна обеспечивать возможность блокировки трафика на основании списков IP-адресов в формате CIDR. | Первый |
| 1.5 | Система должна обеспечивать возможность определения IP-адреса отправителя веб-трафика в случае наличия балансировщиков и прокси-серверов. | Первый |
| 1.6 | Система должна поддерживать следующие режимы защиты:   * активное предотвращение, * обнаружение, * пассивный режим.   Система должна обеспечивать возможность переключения между режимами защиты без прерывания трафика вручную. | Первый |
| 1.7 | Система должна обеспечивать контроль подлинности веб-форм защищаемого приложения с помощью подписи форм. | Второй |
| 1.8 | Система должна обеспечивать возможность маскирования данных в запросах и ответах приложения для защиты от утечек чувствительных данных (персональные данные, данные платежных систем и т.д.) включая защиту от просмотра со стороны администратора WAF. | Второй |
| 1.9 | Система должна предоставлять инструменты для анализа журнала обращений к сайту для выявления и дальнейшего изучения зарегистрированных инцидентов. | Первый |
| 1.10 | Система должна обеспечивать расшифровку SSL/TLS-трафика, возможность загрузки цепочки SSL-сертификатов и SSL-ключей. | Первый |
| 1.11 | Система должна поддерживать следующие технологии уровня приложений:   * HTTP и HTTPS включая SSL v3, TLS v1.0, v1.1, v1.2, v1.3; * WebSocket; * SOAP; * XML и основанные на XML протоколы; * JSON. | Первый |
| 1.12 | Система должна иметь возможность работы в режиме reverse proxy с терминацией SSL/TLS соединения. | Первый |
| 2 | Обнаружение и блокировка атак | 2.1 | Система должна обеспечивать возможность обнаружения и контроля автоматизированной активности через ограничение количества HTTP-запросов. | Первый |
| 2.2 | Система должна обеспечивать возможность модификации ответов от защищаемого веб-приложения путем добавления или замены HTTP-заголовков. | Первый |
| 2.3 | Система должна обеспечивать возможность задания режима принудительного использования протокола HTTPS веб-приложением. | Первый |
| 2.4 | Система должна обеспечивать контроль структуры HTTP-запросов (к защищаемому веб-серверу) на соответствие структуры запроса рабочему предложению RFC 2616 (и RFC 7231 для HTTP) в том числе:   * перечня разрешенных методов HTTP; * максимального количества заголовков HTTP-запроса; * максимальной длины заголовков HTTP-запроса; * максимального размера запроса; * максимального времени ожидания заголовка запроса; * максимального времени ожидания тела запроса; * перечня допустимых типов данных в запросе. | Первый |
| 2.5 | Система должна поддерживать блокировку запросов по версии протокола HTTP. | Первый |
| 2.6 | Система должна обеспечивать защиту от утечек с помощью изменения и перенаправления HTTP-ответов. | Первый |
| 2.7 | Система должна обеспечивать защиту от CSRF (cross-site request forgery) атак путем:   * добавления CSRF-токена к ответам приложения; * обнаружения или блокирования POST-запросов с отсутствующим или неверным CSRF-токеном. | Первый |
| 2.8 | Система должна обеспечивать защиту от SSRF (server-side requst forgery) атак, при которых происходит подмена запросов на стороне сервера. | Первый |
| 2.9 | Система должна обеспечивать обнаружение и блокирование XSS (cross-site scripting) атак, в том числе:   * stored XSS (хранимой XSS); * reflected XSS (отраженной XSS); * DOM-based XSS. | Первый |
| 2.10 | Система должна обеспечивать защиту от внедрения SQL-кода путем обнаружения и блокирования запросов, содержащих легитимные выражения языка SQL и являющихся при этом вредоносными. | Первый |
| 2.11 | Система должна обеспечивать обнаружение и блокирование атак на уязвимости, возникающие при обработке документов в формате XML, путем проверки:   * соответствия XML-сообщения рекомендациям консорциума W3C; * соответствия XML-сообщения формату, заданному в виде схемы XSD; * соответствия запроса описанию сервиса, заданному в виде схемы WSDL; * наличия внешних сущностей и ссылок на них (external entities) в XML-документе; * максимального размера XML-сообщения с учетом уровней вложенности и его структуры. | Первый |
| 2.12 | Система должна обеспечивать обнаружение и блокирование уязвимости открытой переадресации (Open Redirect) в:   * HTTP-заголовке "Location"; * HTML-теге <Meta>; * HTTP-заголовке "Refresh". | Второй |
| 2.13 | Система должна поддерживать "черные" и "белые" списки с типами файлов, загрузка которых блокируется или разрешается. Также должна быть поддержка добавления MIME-типов и расширений в списки. | Первый |
| 2.14 | Система должна обеспечивать возможность антивирусной проверки загружаемых файлов с использованием встроенных и внешних средств антивирусной защиты. | Третий |
| 2.15 | Система должна обеспечивать обнаружение и блокировку атак, направленных на уязвимости набора программ для чтения и редактирования файлов графических форматов ImageMagick. | Первый |
| 2.16 | Система должна иметь возможность проверки ответов приложения на наличие признаков выполнения вредоносного сценария (веб-шелла). | Первый |
| 2.17. | Система должна поддерживать рекурсивное декодирования параметров в запросах, с возможностью задания глубины рекурсии. | Первый |
| 2.18 | Система должна поддерживать механизмы защиты, направленные на предотвращение доступа атакующего к важным файлам защищаемого веб-приложения. | Первый |
| 2.19 | Система должна обеспечивать обнаружение и блокирование компрометации сессии пользователя. Система должна обеспечивать обнаружение признаков кражи сессионного идентификатора пользователя и блокировку попыток доступа с использованием скомпрометированного идентификатора.  Система должна определять смену геолокации или IP-адреса у сессии. | Первый |
| 2.20 | Система должна предотвращать модификации заголовков cookie на стороне клиента путем контроля их неизменности между запросом и ответом с помощью подписи cookie. | Первый |
| 2.21 | Система должна обеспечивать обнаружение сетевых атак, направленных на веб-приложения, посредством сопоставления параметров текущих веб-запросов и их частей с сигнатурами известных атак (база знаний вендора). | Первый |
| 2.22 | Система должна осуществлять контроль автоматизированной активности путем:   * выявления и блокировки запросов роботов и других средств автоматизации, основанный на сигнатурном анализе запросов и эвристическом анализе возможностей клиентского ПО и поведения пользователя на загруженной странице; * контроля доступа легитимных роботов (поисковых систем и т. п.). | Второй |
| 2.23 | Система должна обеспечивать:   * блокировку запросов, параметры которых (IP-адрес, значение заголовков) указаны в репутационных списках; * блокировку доступа к веб-приложению через анонимные сервисы (Tor, VPN, анонимайзеры). | Первый |
| 2.24 | Система должна обеспечивать анализ содержимого JSON-документов в целях исключения потенциально вредоносного содержимого. | Первый |
| 2.25 | Система должна иметь возможность отслеживания попыток доступа пользователя к ресурсам защищаемого веб-приложения на основании применяемых методов аутентификации. | Первый |
| 2.26 | Система должна обеспечивать автоматическое формирование политики безопасного содержимого (content security policy) на основе анализа структуры работы защищаемого приложения с возможностью применения сформированной политики после периода обучения. | Первый |
| 2.27 | Система должна обеспечивать защиту от DDoS-атак уровня приложения путем:   * обнаружения DDoS-атак за счет контроля показателей работы приложения (количество запросов в секунду, количество ошибок сервера и среднее время ответа); * прогнозирования DDoS-атак путем экстраполяции текущих значений контролируемых показателей работы приложения; * ограничения активности групп пользователей с подозрительным поведением. | Второй |
| 2.28 | Система должна обеспечивать возможность добавления сервиса защиты типа CAPTCHA на страницу защищаемого веб-приложения. | Третий |
| 2.29 | Система должна обеспечивать защиту от username enumeration атак (атаки перечислением имен пользователей). | Первый |
| 3 | Динамический анализ уязвимостей | 3.1 | Система должна предоставлять возможность поиска уязвимостей по методу черного ящика для обеспечения:   * сканирования (вручную или по расписанию) защищаемых приложений с помощью графического интерфейса; * получения по результатам сканирования актуального состояния безопасности веб-приложений и использования полученных данных для ручного закрытия найденных уязвимостей и генерации отчетов по уязвимостям. | Первый |
| 3.2 | Система должна обеспечивать возможность обнаружения в пассивном режиме защиты следующих уязвимостей:   * ошибки конфигурации веб-сервера; * уязвимости в логике работы приложения; * раскрытие чувствительной информации (конфигурационных файлов, директорий приложения на сервере); * ошибки выполнения сценариев на сервере и ошибки обращения к базам данных. | Первый |
| 4 | Работа с правилами и политиками безопасности | 4.1 | Система должна обеспечивать возможность обнаружения признаков атак на веб-приложения и регистрации событий безопасности на основе установленных правил. | Первый |
| 4.2 | Система должна содержать набор предустановленных правил обработки сетевого трафика и переопределения реакции на такие атаки, как:   * направленные на контроль эксплуатации уязвимостей из списка CVE; * направленные на проверку загружаемых файлов; * реализующие защиту от атак, направленных на внедрение небезопасного кода; * репутация IP-адреса; * направленные на проверку JSON Web Token (JWT); * направленные на защиту от IDOR атак; * направленные на защиту от атак, реализуемых путем перебора УЗ. | Первый |
| 4.3 | Система должна поддерживать правила обработки трафика, настроенные на защиту веб-приложений на базе следующих технологий:   * .NET * Java * Microsoft Exchange * Node.js * PHP * Bitrix | Первый |
| 4.4 | Система должна обеспечивать возможность кастомизации предустановленных правил. | Первый |
| 4.5 | Система должна обеспечивать возможность создания, изменения, удаления пользовательских правил и поддерживать регулярные выражения. | Первый |
| 4.6 | Система должна поддерживать следующие стандартные действия с правилами:   * блокировки веб-приложений; * запись информации о событиях в базу данных Системы; * отправлять информацию об обнаруженных событиях безопасности на syslog-сервер. | Второй |
| 4.7 | Системе должна обеспечивать возможность группировки предустановленных и пользовательских правил. | Первый |
| 4.8 | Система должна обеспечивать возможность создания исключений для правил. | Первый |
| 4.9 | Система должна обеспечивать возможность точечной настройки политик администратором Системы, используемых для конфигурации модулей защиты и правил, как для отдельных приложений, так и для нескольких приложений одновременно. | Первый |
| 4.10 | Система должна обеспечивать возможность создания шаблонов политик безопасности на основе предустановленных и пользовательских правил. Система должна содержать предустановленные шаблоны политик безопасности для распространенных веб-приложений, таких как IIS, Bitrix. | Первый |
| 4.11 | Система должна обеспечивать возможность обновления (дополнения) списка обнаруживаемых заголовков User-Agent в правилах. | Второй |
| 5 | Настройка и управление системой | 5.1 | Система должна обеспечивать возможность управления через:   * консольный интерфейс (доступный по протоколу SSH), или * графический интерфейс (веб-интерфейс, доступный по протоколу HTTPS). | Первый |
| 5.2 | Система должна обеспечивать возможность просмотра информации о событиях (инцидентах, атаках, уязвимостях). Информация должна быть представлена как в краткой, так и полной форме. | Первый |
| 5.3 | Система должна иметь следующие механизмы управления событиями:   * сортировку по любому из отображаемых атрибутов событий; * фильтрацию по любому из отображаемых атрибутов событий; * многоуровневую агрегацию (группировку событий с одинаковыми значениями атрибутов); * корреляцию (группировку взаимосвязанных событий и выявление комплексных атак с использованием предустановленных правил и (или) правил, созданных пользователем). | Первый |
| 5.4 | Система должна обновлять данные о событиях в автоматическом и ручном режиме. | Второй |
| 5.5 | Система должна обеспечивать предоставление следующей информации об атаке:   * информацию об источнике атаки:   + IP-адрес и порт;   + информацию о местоположении (страна, регион, город);   + версию ОС и браузера;   + полный перечень параметров и заголовков запроса и их значений;   + имя пользователя в приложении (если известно);   + тело запроса; * информацию о цели атаки:   + IP-адрес и порт;   + Hostname атакуемого;   + идентификатор защищаемого приложения;   + адрес, на который направлена атака (URL);   + полный перечень заголовков ответа;   + код состояния, содержимое и время ответа; * информация о событии:   + уникальный идентификатор события;   + идентификатор сработавшего модуля защиты;   + описание атаки;   + основополагающий признак атаки (параметр запроса или ответа);   + действия, выполненные по результатам атаки;   + уровень опасности.   Полный список атрибутов атаки должен быть уточнен Исполнителем на этапе планирования и проектирования Системы. | Первый |
| 5.6 | Система должна обеспечивать определение уровня опасности событий и возможность выполнения различных действий с событиями каждого уровня. Например:   * Высокий уровень: выполнение блокировки, оповещение о возникновении события, логирование события. * Средний уровень: оповещение о возникновении события, логирование события. * Низкий уровень: логирование события. | Первый |
| 5.7 | Система должна обеспечивать предоставление следующей информации об уязвимостях:   * идентификатор уязвимости; * статус; * уровень опасности; * описание и ссылка на описание уязвимости из базы знаний вендора; * источник уязвимости; * количество событий разного уровня важности в корреляции; * дата и время обнаружения уязвимости и выполнения последней проверки наличия уязвимости.   Полный список атрибутов уязвимости должен быть уточнен Исполнителем на этапе планирования и проектирования Системы. | Первый |
| 5.8 | Система должна обеспечивать хранение информации об атаках в формате XML и JSON для дальнейшего анализа. | Первый |
| 5.9 | Система должна предоставлять программный интерфейс (REST API, RESTfull API или аналогичный) для автоматизации задач по управлению системой с помощью внешних программных средств. | Первый |
| 5.10 | Система должна обеспечивать возможность проверки регулярных выражений для их дальнейшего использования при настройке правил, действий и модулей защиты. | Первый |
| 5.11 | Система должна обеспечивать возможность импорта и экспорта данных конфигурации и политик безопасности. | Первый |
| 5.12 | Система должна предоставлять информационную панель (дашборд) с полным списком событий безопасности (атаки, инциденты, уязвимости, информационные события), а также сводную информацию об атаках в виде графиков, гистограмм и карт.  Полный список дашбордов должен быть уточнен Исполнителем на этапе планирования и проектирования Системы. | Первый |
| 5.13 | Система должна обеспечивать возможность настройки дашбордов. | Первый |
| 5.14 | Система должна позволять обновлять данные о событиях на дашбордах через определенные промежутки времени. | Первый |
| 5.15 | Система должна обеспечивать возможность формирования отчетов, вручную или по расписанию с возможностью выгрузки в форматах PDF, HTML, DOCX или CSV. | Первый |
| 5.16 | Система должна обеспечивать возможность формирования отчетов по:   * атакам; * инцидентам; * уязвимостям; * IP адресам; * временным интервалам.   Полный список отчетов должен быть уточнен Исполнителем на этапе планирования и проектирования Системы. | Первый |
| 5.17 | Система должна обеспечивать возможность отправки уведомлений об инцидентах по электронной почте. | Первый |
| 5.18 | Система должна обеспечивать возможность онлайн- и офлайн-обновления программных компонентов и сигнатур атак бесперебойно (без остановки сервиса). Должна быть возможность запуска обновления программных компонентов в ручном режиме для оптимального выбора времени обновления. База знаний и правил защиты от вендора должны обновляться в автоматическом режиме.  Обновление должно происходить без потери правил и исключений. | Первый |

Требования должны быть уточнены Исполнителем и согласованы Заказчиком на этапе проектирования и планирования системы.

## Функционально-ролевая модель

В Системе должна быть реализована ролевая модель доступа, обеспечивающая возможность разграничения доступа пользователей к объектам Системы и разрешения или запрета выполнения определенных действий. Также ролевая модель доступа должна обеспечивать возможность разрешения или запрета доступа пользователей к информации и настройкам Системы.

Требования к ролям и выполняемым функциям в Системе описаны в таблице 4.

Таблица 4 - Функционально-ролевая модель

|  |  |  |
| --- | --- | --- |
| **п.п** | **Роль** | **Функции** |
| 1 | Администратор | Полный доступ ко всем сущностям и настройкам системы (политики, шаблоны политик, правила, шаблоны правил, отчеты, дашборды, конфигурация, запуск обновлений); реагирование на атаки (блокировка атак, изменение уровня опасности атак). |
| 2 | Администратор ИБ | Полный доступ к политикам, шаблонам политик, правилам, шаблонам правил, отчетам, дашбордам, реагирование на атаки (блокировка атак, изменение уровня опасности атак). |
| 3 | Аудитор ИБ | Доступ на чтение к общим сущностям системы:   * просмотр инцидентов ИБ; * просмотр дашбордов и отчетов; * просмотр информации о системе.    Доступ на создание:   * персональных дашбордов; * отчетов, с возможностью выгрузки. |

Прочие требования к функциям ролей должны быть уточнены Исполнителем и согласованы Заказчиком на этапе проектирования и планирования системы.

## Требования к методологической проработке

Должен быть подготовлен методический документ, описывающий процесс публикации веб-приложений с использованием WAF.

### Общие требования к интеграции с существующими системами

Решения о необходимости реализации конкретных интеграционных потоков для каждой смежной системы должны быть приняты в рамках работ по проектированию системы.

Работы по тестированию интеграционных связей между системой и интегрируемыми информационными системами, должны быть запланированы в рамках работ по проектированию системы и учтены в календарном плане проекта.

Прочие требования (в т. ч. список интегрируемых систем) должны быть уточнены Исполнителем на этапе проектирования и планирования системы.

### Требования к взаимодействию со смежными системам

Система должна иметь возможность интеграции c:

* системой управления событиями информационной безопасности (SIEM) через системный журнал (syslog в формате CEF) или пользовательские коннекторы в части передачи информации об обнаруженных атаках;
* системой оркестрации, автоматизации и реагирования на инциденты (SOAR) через API в части инициирования управляющих или блокирующих действий;
* системами антивирусной защиты или системами защиты от таргетированных атак, поддерживающими интеграцию через ICAP, для проверки входящих и исходящих файлов на наличие вредоносного содержимого;
* электронной почтой через SMTP для оповещения пользователей об обнаруженных атаках;

Требования к взаимодействию со смежными системами (в т. ч. список интегрируемых систем) должны быть разработаны в рамках работ по проектированию системы и учтены в календарном плане проекта.

### Требования к доработке в интегрируемых системах

В случае необходимости внесения изменений в интегрируемые ИС, Исполнитель предоставляет Заказчику перечень необходимых изменений и предполагаемые средства реализации. Исполнитель совместно с Заказчиком и Владельцами ИС определяет возможность внесения изменений в интегрируемые ИС и определяет сроки реализации изменений.

Выполнение изменений в интегрируемых ИС выполняет Заказчик.

В случае невозможности реализации изменения, Исполнитель выносит на УК предложение об исключении данной функциональности из объема проекта.

Требования к доработке в интегрируемых системах должны быть уточнены Исполнителем на этапе проектирования и планирования системы.

## Требования к архитектуре системы

### Требование к проектированию архитектуры

Предлагаемое решение должно являться полностью локальным, установка всех своих компонентов должна осуществляться непосредственно на площадках Заказчика, без передачи какой-либо информации в облачные сервисы.

Компоненты Системы размещаются в корпоративной сети после модуля межсетевого экранирования и внешнего балансировщика в демилитаризованной зоне.

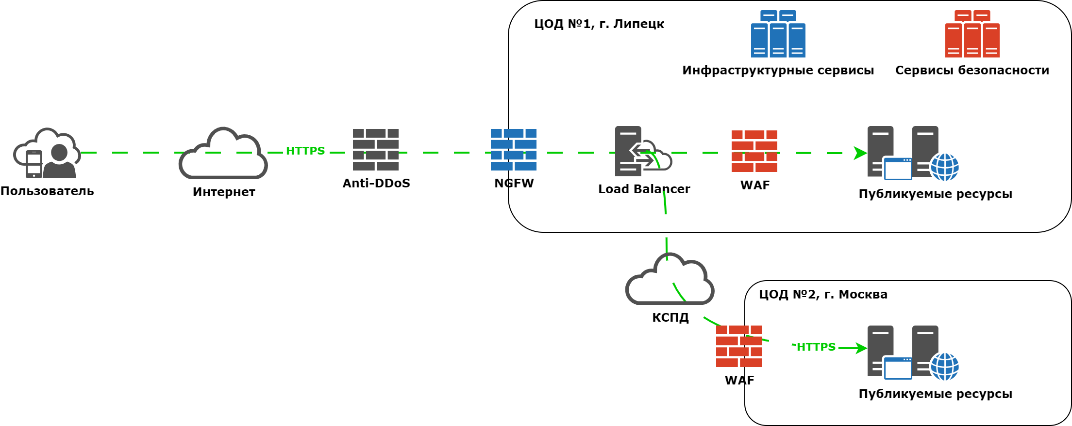
Сервера публикуемых ресурсов должны размещаться после Системы таким образом, что внешний веб-трафик, поступающий из сети Интернет в сторону публикуемых сервисов, предварительно проходил проверку DDoS-защиты, далее попадал на межсетевые экраны периметра, где осуществляется первичный анализ и фильтрация, далее данный трафик поступал на интерфейс внешнего балансировщика (Citrix), где осуществляется непосредственно публикация информационных ресурсов, и далее передавался на интерфейсы Системы для анализа атак, специфичных для протоколов и логики веб-приложений. После осуществления анализа, в соответствии с настройками балансировки нагрузки, трафик доходит до сервера веб-приложений.

В состав системы должны входить:

* консоль управления в виде веб-интерфейса для взаимодействия с пользователями и администраторами системы;
* интерфейс для взаимодействия с внешними системами автоматизации (REST API) и документация к нему;
* внутренние сервисы для управления конфигурацией, выполнения периодических задач, мониторинга и поддержания работы всех составляющих системы;
* базы данных и системы хранения для конфигурации, информации о событиях безопасности и действиях пользователей системы, отчетов и резервных копий данных;
* сервисы, отвечающие за обработку защищаемого трафика.

Концептуальная архитектура Системы изображена на рисунке 2.

Рисунок 2 - Концептуальная архитектура



Прочие требования должны быть уточнены Исполнителем на этапе реализации проекта.

## НЕФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ К СИСТЕМЕ

## Требования к расширяемости и масштабируемости

Система в целом, должна обеспечивать возможность вертикального и горизонтального масштабирования при увеличении количества интегрируемых информационных систем или объектов управления, средствами используемого базового программного обеспечения.

Оборудование и системное программное обеспечение, должно обеспечивать возможность вертикального и горизонтального масштабирования при увеличении количества интегрируемых информационных систем или объектов управления.

Оборудование должно обеспечивать возможность увеличения производительности, путем наращивания числа функциональных блоков (процессорные ядра, оперативная память, сетевые интерфейсы, система хранения данных), выполняющих одни и те же задачи, без необходимости фундаментальной перестройки архитектуры информационной системы.

Процедура масштабирования должна быть описана в документе «Регламент масштабирования» проекта. Алгоритм действий для вертикального и горизонтального масштабирования должен быть доработан в процессе реализации проекта Исполнителем.

Прочие требования к масштабированию системы должны быть уточнены Исполнителем на этапе реализации проекта.

## Требования к надежности системы

В системе должны быть использованы следующие способы повышения надежности:

* Резервирование программно-технических средств;
* Диагностика технических средств и программного обеспечения;
* Защита данных, программного обеспечения и технических средств от несанкционированного вмешательства;

Надежность системы должна характеризоваться следующими значениями показателей:

* Время восстановления работоспособного состояния компонентов системы в случае аварии не более в соответствии с классом критичности Системы – Business Critical;
* Отказом системы следует считать прекращение выполнения одной из основных функций в соответствии с заданными к ним требованиями;

Прочие требования к надежности системы, должны быть уточнены Исполнителем на этапе проектирования и планирования системы.

## Требования к мониторингу системы

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.

Должно обеспечиваться отслеживание статуса применения конфигурации.

В рамках проекта Исполнителем должны быть сформулированы и согласованы с Заказчиком основные метрики мониторинга производительности и доступности.

Необходимость постановки Системы на мониторинг в ситуационный центр ИТ ([HotLine](https://confluence.nlmk.com/pages/viewpage.action?pageId=116515123" \l ":~:text=%D0%9E%D0%BF%D0%B5%D1%80%D0%B0%D1%82%D0%BE%D1%80-,HotLine,-%D0%93%D1%80%D1%83%D0%BF%D0%BF%D0%B0%20%D1%81%D0%BE%D1%82%D1%80%D1%83%D0%B4%D0%BD%D0%B8%D0%BA%D0%BE%D0%B2%2C%20%D1%80%D0%B0%D0%B1%D0%BE%D1%82%D0%B0%D1%8E%D1%89%D0%B0%D1%8F)) должны быть уточнены Исполнителем на этапе проектирования и планирования системы.

Прочие требования к мониторингу системы должны быть уточнены Исполнителем на фазе проектирования и планирования системы.

### Мониторинг инфраструктуры

Мониторинг инфраструктурных метрик должен выполняеться существующей системой мониторинга Zabbix с визуализацией в Grafana.

Мониторинг выполняется для инфраструктурных метрик:

* Утилизация ресурсов – ЦПУ, ОЗУ, дисков, сетевых интерфейсов;
* Сетевая доступность.

Дополнительных требований к мониторингу инфраструктурных метрик таких виртуальных машин в рамках проекта не предъявляется.

## Требования к производительности

Система должна соответствовать требованиям в части показателей назначения, которые перечислены в таблице 5.

Таблица 5 - Требования к производительности

|  |  |  |
| --- | --- | --- |
| **п.п.** | **Параметр** | **Значение** |
| 1 | Пропускная способность инспектируемого Интернет трафика | 1 Гбит/c |
| 2 | Количество запросов, которое может обработать сервер в одну секунду (RPS) | от 2000 (минимум) |
| 3 | Количество пользователей, одновременно работающих с системой в единицу времени | не менее 10 |
| 4 | Время отклика административных консолей, не более | 1 секунда |
| 5 | Допустимое время простоя системы в год, час | 86,4 |
| 6 | Допустимое время простоя системы в месяц, час | 7,20 |
| 7 | Допустимое время простоя системы в неделю, час | 1,68 |
| 8 | Нормальный режим функционирования Системы | 24\*7\*365 |
| 9 | Коэффициент доступности системы | 99 % |
| 10 | Срок хранения исторических данных | не менее 1 мес. |
| 11 | Запас роста | 25% |
| 12 | RPO (recovery point objective) это максимальный период времени, за который могут быть потеряны данные в результате инцидента (Продуктивная среда). | 8 ч. |
| 13 | RTO (recovery time objective) это промежуток времени, в течение которого система может оставаться недоступной в случае аварии (Продуктивная среда). | 8 ч. |

Прочие требования к производительности должны быть уточнены Исполнителем на этапе реализации проекта.

## Требование к лингвистическому обеспечению

Основной язык в интерфейсах всех подсистем – Русский (пользовательский).

Дополнительный язык и в интерфейсах всех подсистем – Английский (пользовательский).

Основной язык интерпретации событий журналов подсистем – Английский.

Дополнительный язык интерпретации событий журналов подсистем – Русский.

## Требования к технологическому стеку

Для реализации своих функций система, вне зависимости от выбранного варианта размещения должна максимально использовать готовые программные компоненты, существующие на рынке.

Системное ПО должно включать ПО следующих видов:

* Операционная система;
* Программное обеспечение серверов приложений;
* Программное обеспечение организации кластеров (если используются).

Для реализации функциональности системы должно использоваться программное обеспечение, представленное в таблице 6.

Таблица 6 - Требования к технологическому стеку.

|  |  |  |
| --- | --- | --- |
| **п.п.** | **Наименование подсистемы** | **Требование к программному обеспечению** |
| 1. | Платформа контейнеризации | Kubernetes (k8s) или OKD |
| 2. | Операционные системы | Microsoft Windows Server актуальной версии или Red OS (РЕД ОС) актуальной версии  Использование других ОС отдельно согласовывается с Заказчиком  Версии и редакции ОС необходимо согласовать на этапе проектирования |
| 3. | СУБД | Для стека Windows - MSSQL (может быть предоставлено «as a service»)  Для стека Linux – PostgreSQL (может быть предоставлено «as a service»)  Прочие СУБД требуют отдельного согласования.  Версии и редакции СУБД необходимо согласовать на этапе проектирования |

Прочие требования к технологическому стеку должны быть уточнены Исполнителем и согласованы Заказчиком на этапе проектирования.

## Требования к комплекту поставки

В рамках проекта, Исполнитель разрабатывает и согласовывает с Заказчиком детальный план-график поставки программного обеспечения.

Всё программное обеспечение Системы должно содержать комплект соответствующих лицензий на его использование. Все поставляемое программное обеспечение должно быть обеспечено технической документацией на русском языке.

Все поставляемое программное обеспечение должно быть обеспечено сертификатами и другими необходимыми документами в соответствии с действующим законодательством Российской Федерации.

## Требования к структуре команды

В рамках реализации проекта от Исполнителя требуется опыт внедрения, модернизации и поддержки системы класса WAF в компаниях с аналогичным организационным и технологическим ландшафтом от 2-х лет.

Исполнитель должен иметь опыт успешной реализации аналогичных проектов. Аналогичным является проект, соответствующий данным ФТТ по показателям:

объём проекта;

* функциональные требования;
* технические требования;
* требования к миграции;
* требования информационной безопасности;
* сроки реализации.

Подтверждение опыта успешной реализации проектов должно быть предоставлено по запросу Заказчика в форме, согласованной с Заказчиком (сертификация Исполнителя как партнёра вендора, документальное подтверждение, референс-визит, очная встреча, онлайн-конференция или другая форма).

Специалисты проектной рабочей группы Исполнителя должны обладать подтвержденной квалификацией и опытом участия в успешной реализации аналогичных проектов.

Технические специалисты проектной рабочей группы Исполнителя должны быть сертифицированы по программам сертификации производителей ПО и оборудования, включенных в проект (обладать сертификатами вендора о прохождении обучения по внедрению/эксплуатации/администрированию WAF). При отсутствии у производителей программ сертификации допускается другая форма подтверждения квалификации по согласованию с Заказчиком (опыт участия в аналогичных проектах, пройденное обучение специалистов проектной рабочей группы Исполнителя и др.).

Примерный перечень специалистов, которые должны быть включены в проектную рабочую группу Исполнителя:

* Руководитель (менеджер) проекта;
* Архитектор проекта;
* Технический писатель;
* Технический специалист по серверному оборудованию и/или платформе виртуализации;
* Технический специалист по WAF (инженер внедрения WAF), внедряемой в рамках проекта с опытом внедрения, модернизации и поддержки систем класса WAF от 2-х лет;
* Технический специалист по сетевым технологиям;
* Архитектор информационной безопасности с опытом внедрения, модернизации и поддержки систем класса WAF от 2-х лет;
* Технический специалист по резервному копированию.

Количество специалистов (FTE) должно быть достаточно для выполнения всех задач проекта в соответствии с графиком проекта. Для технических специалистов допускается совмещение ролей.

Технические специалисты должны быть выделены на проект на 100% рабочего времени.

Состав проектной рабочей группы специалистов Исполнителя должен быть согласован с Заказчиком.

Любые изменения в составе рабочей группы должны быть согласованы с Заказчиком.

В случае замены специалиста в рабочей группе Исполнитель должен обеспечить передачу новому специалисту информации по текущему статусу проекта для минимизации времени «погружения» в проект. Замена специалиста Исполнителя не должна влиять на график проекта.

Прочие требования к Исполнителю и рабочей группе будут определены Договором на проведение работ.

## ТРЕБОВАНИЯ К ИТ-ИНФРАСТРУКТУРЕ

## Общие требования к системе

Система должна представлять собой программно-аппаратный комплекс и поддерживать следующие режимы работы:

* режим обратного прокси-сервера (reverse proxy) — соединение в разрыв, в котором WAF выступает в качестве прокси-сервера между клиентом и защищаемым веб-приложением;
* режим сниффера (sniffer) — подключение через SPAN-порт, при котором WAF выполняет анализ копии входящего и исходящего трафика;
* режим прозрачного прокси-сервера (transparent proxy) — соединение в разрыв, при котором WAF фильтрует выбранный трафик, а остальные данные передаются по мосту L2 без обработки;
* режим моста (L2 bridge) — соединение в разрыв с использованием моста L2, при котором трафик прозрачно проходит через WAF от клиента к защищаемому серверу, что позволяет обнаруживать угрозы, при этом, не влияя на работу защищаемого приложения;
* автономный (forensics) — офлайн-анализ журналов веб-сервера и сетевых дампов для обнаружения следов атак.

Система должна обеспечивать возможность модернизации путем расширения состава программных средств в случае увеличения объема трафика и количества защищаемых веб-приложений.

Система должна функционировать в следующих режимах:

* штатный режим;
* сервисный режим;
* аварийный режим.

В штатном режиме функционирования Система должна обеспечивать выполнение заявленных функций в полном объеме.

В сервисном режиме функционирования Система должна обеспечивать возможность обновления программного обеспечения (далее – ПО) Система, а также функции диагностики и анализа работоспособности WAF для проведения работ по обслуживанию, устранению неисправностей и модернизации Системы.

В аварийном режиме функционирования допускается полная или частичная потеря работоспособности Системы, при этом не должно оказываться влияние на функционирование информационных систем Заказчика. Должен быть предусмотрен комплекс мероприятий по восстановлению работоспособности WAF, обнаружению и устранению причин перехода Системы в аварийный режим.

Система должна быть реализована в отказоустойчивой конфигурации по схеме Active — Passive в 2-х георазделенных ЦОД-ах и предполагает схему Основной-Резервный ЦОД.

Система должна обеспечивать возможность резервного копирования и восстановления данных конфигурационных файлов и данных в случаях аварийных ситуаций либо несанкционированных воздействий на элементы Системы.

Требования к стандартизации и унификации

Аппаратное и программное (системное) обеспечение системы, должно соответствовать требованиям промышленных стандартов и требованиям нормативной документации ПАО «НЛМК» (Техническая политика в области ИТ). При создании системы необходимо использовать серийное оборудование, типовые программные решения и программные средства.

Прочие требования к стандартизации и унификации должны быть уточнены Исполнителем на этапе реализации проекта.

## Требования к размещению

Распределение компонентов Системы по площадкам и сегментам должно осуществляться в соответствии с таблицей 7.

Таблица 7 - Распределение и наименование компонентов

|  |  |  |
| --- | --- | --- |
| п.п. | Наименование предприятия и адрес объекта | Наименование компонента |
| 1 | ПАО «НЛМК» – г. Липецк, пл. Металлургов, д. 2 | Узел управления и узлы обработки |
| 2 | ПАО «НЛМК» – г. Москва, Чермянский пр-д, д. 5А, стр. 1 | Узел управления и узлы обработки |

Размещение на выделенных серверах должно быть проработано и согласовано в рамках проектирования, включая следующие пункты:

* Обоснование размещения на выделенных физических серверах;
* Локация (место установки) физических серверов;
* Спецификация оборудования;
* Зоны ответственности по поддержке оборудования.

## Требования к сетевому сегментированию

В рамках проекта должна быть определена необходимость сетевого сегментирования и выделения компонентов системы (подсистем) в отдельную область безопасности (отдельный VLAN).

Перечень сетевых сегментов и правила сетевого взаимодействия должны быть приведены в Проектном решении.

Прочие требования должны быть уточнены Исполнителем на этапе проектирования и планирования системы.

## Требования к резервному копированию

### Общие требования

Резервное копирование компонентов, развернутых в соответствии с требованиями к технологическому стеку инфраструктуры, выполняется существующей системой резервного копирования согласно регламенту резервного копирования (Приложение В), в ином случае методы резервного копирования Системы должны быть разработаны Исполнителем на этапе проектирования Системы и согласованы с Заказчиком.

### Прочие компоненты системы

Для компонентов, не соответствующих требованиям к технологическому стеку, в рамках проекта Исполнителем должны быть сформулированы и согласованы с Заказчиком требования к резервному копированию системы.

Все компоненты системы должны быть поставлены на резервное копирование Заказчиком, в соответствии с разделом документа «Проектное решение» - «Резервное копирование и восстановление системы».

Подсистема резервного копирования должна обеспечивать сохранение всей информации, хранимой на серверах системы, в том числе:

* Любых файлов файловой системы серверов;
* Текущего состояния и настроек операционных систем всех серверов;
* Файлов табличных пространств СУБД;
* Файлов инициализации и управляющих параметров СУБД;
* Файлов активных и архивных журналов;
* Текущего состояния, настроек и внутренних данных используемого прикладного ПО.

Настройку существующей системы резервного копирования Заказчика для выполнения процедур резервного копирования системы выполняет Заказчик в соответствии с проектными решениями.

Прочие требования к резервному копированию системы должны быть уточнены Исполнителем на этапе проектирования и планирования системы.

## Инфраструктурные требования к организационному обеспечению

### Инфраструктурные требования к Проектному решению на систему

В рамках выполнения проекта Исполнителем должен быть разработан и согласован с Заказчиком документ «Проектное решение». Степень детализации документа – высокая (Step-by-Step). Документ «Проектное решение» готовится в формате, утвержденном Заказчиком.

Основные требования к документу приведены в Приложении А. Прочие требования к проектному решению на систему должны быть уточнены Исполнителем на этапе проектирования и планирования системы.

### Инфраструктурные требования к проверке производительности

В ходе реализации проекта, перед переходом к промышленной эксплуатации, Исполнитель совместно с представителями Заказчика должен провести проверку производительности системы с подтверждением основных показателей производительности. Проверка должна производиться путем нагрузочного тестирования системы.

Прочие требования к проверке производительности системы должны быть уточнены Исполнителем на этапе проектирования и планирования системы.

### Требования к проверке состояния здоровья системы

После создания системы Исполнителем должна быть проведена процедура проверки журналов системы на наличие ошибок и предупреждений. Данное мероприятие должно быть проведено для проверки правильности конфигурирования системы и отсутствия проблем и ошибок.

Результатом выполнения процедуры должен являться оформленный Исполнителем и согласованный с Заказчиком отчет, содержащий сведения о соответствии конфигурации системы рекомендуемой.

Прочие требования к проверке состояния здоровья системы должны быть уточнены Исполнителем на этапе проектирования и планирования системы.

### Требования к плану восстановления системы

В ходе реализации проекта Исполнителем должны быть определены основные скрипты сбоя системы и регламент аварийного восстановления, описанные в документе «Инструкция администратора».

Должны быть учтены следующие сценарии сбоя:

* Выход из строя одного сервера;
* Выход из строя всех серверов;
* Необратимые изменения БД;
* Повреждение, удаление, изменение любого из объектов БД;
* Выход из строя СХД;

Степень детализации скриптов – высокая (Step-by-Step).

Прочие требования к скриптам и регламенту аварийного восстановления системы, должны быть уточнены Исполнителем на этапе проектирования и планирования системы.

## Класс критичности создаваемой системы

Система должна отвечать требованиям высокой доступности в соответствии с классом критичности системы, описанным в таблице 8.

Таблица 8 - Требования к доступности

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **п.п.** | **Класс критичности** | **Доступность (%)** | **Максимальное суммарно возможное время простоя в год (час)** | **Требования** |
| 1 | Business Critical | 99,0 | 86,4 | Аппаратная отказоустойчивость серверных компонентов ядра системы обеспечиваются кластерной инсталляцией в 2-х разделенных ЦОД  В рамках проекта Исполнителем должна быть реализована высокая доступность (программная и аппаратная отказоустойчивость) для всех компонентов продуктивной среды. Решения по высокой доступности (кластер, ферма, реплика, пр.) должны быть согласованы с Заказчиком. |

Прочие требования к доступности системы должны быть уточнены Исполнителем на этапе реализации проекта.

## ТРЕБОВАНИЯ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В системе предусматривается обработка информации, составляющей коммерческую тайну.

Требования по информационной безопасности распространяются на все субъекты доступа к системе (пользователей и администраторов), а также должны реализовываться всеми компонентами системы.

При реализации требований по информационной безопасности должны использоваться встроенные возможности и механизмы защиты информации операционных систем, систем управления базами данных, прикладного программного обеспечения, средств виртуализации, средств контейнеризации и других компонентов системы. В случаях, если выполнение требований по информационной безопасности не реализуемо с помощью встроенных механизмов должны применяться дополнительные наложенные средства защиты информации.

Требования по обеспечению целостности и доступности предъявляются ко всем информационным ресурсам (далее – ИР) системы, требования по обеспечению конфиденциальности – к информации ограниченного доступа, обрабатываемой системой, а также к настройкам средств защиты информации и журналам аудита событий информационной безопасности.

В рамках проекта должны реализовываться меры по обеспечению безопасности информации, составляющей коммерческую тайну.

Система должна реализовывать следующие функции информационной безопасности:

* функции управления доступом;
* функции регистрации и учета;
* функции обеспечения целостности;
* функции криптографической защиты.

Детальные требования к функциям безопасности приведены далее в документе.

## Требования к функциям управления доступом

В системе должны быть реализованы следующие функции управления доступом:

* контроль (предоставление/отказ) доступа пользователей на основании разработанной в рамках проекта ролевой модели, в которой должны быть описаны все необходимые варианты доступа и роли пользователей в системе. Ролевая модель, разрабатываемая в рамках проекта, должна основываться на принципах минимально необходимых и достаточных полномочий и непротиворечивости ролей (как минимум должны быть определены следующие роли в системе: администратор системы и аудитор информационной безопасности);
* идентификация и аутентификация субъектов доступа при доступе к Системе с использованием службы каталогов Microsoft Active Directory. Для отдельных субъектов доступа (администраторов ОС, СУБД или сервисные/технические учетные записи, используемые системой в автоматическом режиме) допускается реализация схемы аутентификации на основании пароля условно-постоянного действия. Использование данной схемы аутентификации должно быть обосновано в рамках проектного решения. Требования к паролям должны соответствовать правилам парольной защиты в ПАО «НЛМК»;
* ограничение количества неуспешных попыток доступа к системе, после которых блокируется учетная запись пользователя. Количество неуспешных попыток доступа, а также обоснование невозможности реализации данного требования для отдельных категорий субъектов доступа должны быть приведены в рамках проектного решения;
* возможность контроля доступа к ресурсам системы на сетевом уровне;
* возможность ограничения на работу пользователя в системе в рамках более чем в одной сессии;
* доступ к системе должен быть разрешен только через корпоративную сеть Заказчика.

Регистрация и работа пользователей в системе должна осуществляться с учетом всех норм, правил и требований "Положения о процессе управления доступом".

В проектном решении должна быть отражена информация о сервисных/технических учетных записях и их полномочиях, создаваемых в системе для организации интеграционных взаимодействий со смежными системами.

Любое назначение прав в Системе должно выполняться явным образом: либо путем прямого предоставления отдельных прав конкретному пользователю, либо через включение в группу/назначение роли, обладающей набором необходимых привилегий. При создании нового пользователя в Системе, ему не должны автоматически назначаться какие-либо права доступа без явного их назначения администратором.

Прочие требования к функциям управления доступом должны быть уточнены Исполнителем на этапе реализации проекта.

## Требования к функциям регистрации и учета

Для реализации функций регистрации и учета событий информационной безопасности должны использоваться встроенные средства системы.

Система должна аккумулировать регистрируемые события, сохраняя их в соответствующих таблицах базы данных и/или логах. Доступ к указанным таблицам базы данных и/или логам должен быть ограничен для всех ролей за исключением роли Администратор информационной безопасности.

Регистрации подлежат следующие события:

* регистрация входа (выхода) пользователей в систему (из системы). В параметрах регистрации должно указываться:
  + дата и время входа (выхода) пользователей в систему (из системы);
  + идентификатор пользователя, предъявленный при запросе доступа;
  + результат попытки входа: успешная или неуспешная (несанкционированная);
  + идентификатор (адрес) точки, с которой осуществлялся вход в Систему.
* регистрация назначения/изменения полномочий субъектов доступа. В параметрах регистрации должно указываться:
  + дата и время изменения полномочий доступа;
  + результат попытки изменения полномочий: успешная или неуспешная (несанкционированная);
  + идентификатор пользователя (процесса) осуществившего изменение;
  + прежнее и измененное значение полномочий доступа.
* регистрация попыток доступа к защищаемым информационным ресурсам внутренними средствами Системы. В параметрах регистрации должно указываться:
  + дата и время попытки доступа к защищаемому ресурсу;
  + результат попытки доступа: успешная или неуспешная (несанкционированная);
  + идентификатор субъекта доступа;
  + спецификация защищаемого информационного ресурса.
* регистрация действий пользователей и администраторов в Системе. В параметрах регистрации должно указываться:
  + дата и время регистрируемого события;
  + идентификатор (код) субъекта доступа;
  + идентификатор (код) объекта доступа;
  + выполняемое действие.
* регистрация события формирования и вывода на экран, экспорта из системы документов с использованием средств прикладного программного обеспечения. Должна обеспечиваться регистрация следующих событий:
  + дата и время запуска программного средства, с помощью которого формировался/экспортировался документ;
  + идентификатор пользователя, запустившего программное средство;
  + информация о сформированном документе.

Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения. Минимальный срок хранения событий журналов безопасности должен составлять 3 месяца.

Система должна обеспечивать возможность передачи событий в SIEM систему Заказчика в автоматизированном режиме.

В рамках проекта должны быть проработаны решения по способу передачи данных в SIEM, описание типов передаваемых событий ИБ (с указанием уникальных идентификаторов событий), а также правила нормализации передаваемых событий. В проектном решении также должна быть отражена следующая информация:

* полный перечень оборудования и устанавливаемого программного обеспечения (включая общесистемное ПО), подключаемого к SIEM;
* соответствующие оборудованию сетевые адреса и сегменты сети;
* обоснование исключения тех или иных источников событий из перечня подключаемых источников;
* настойки журналирования, способы и пути хранения событий ИБ;
* оценочный размер передаваемых журналов событий.

В случае, если прикладное программное обеспечение не содержит механизмов для реализации тех или иных требований Исполнителем должны быть организованы работы по доработке прикладного программного обеспечения. При невозможности доработки прикладного программного обеспечения Исполнителем должны быть предложены решения по реализации требований с использованием наложенных средств защиты информации.

Прочие требования к функциям управления доступом должны быть уточнены Исполнителем на этапе реализации проекта.

## Требования к функциям обеспечения целостности

В системе должна обеспечиваться целостность программной среды.

## Требования к функциям криптографической защиты информации

Криптографическая защита должна исключать возможность получения несанкционированного доступа к защищаемой информации и должна обеспечивать:

* шифрование конфиденциальной информации системы при её передаче по открытым каналам связи;
* шифрование данных аутентификации пользователей системы;
* запрет хранения паролей в системе в открытом виде.

## Защита технических средств, систем связи и передачи данных

В Системе должны обеспечиваться следующие функции:

* контроль и управление доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования Системы, в помещения и сооружения, в которых они установлены;
* размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

Защита технических средств должна обеспечиваться организационными мерами на объектах внедрения силами Заказчика.

Обеспечение сетевой безопасности при взаимодействии с другими информационными системами должно отвечать предъявляемым требованиям к обеспечению безопасности периметра корпоративной сети (периметра информационной безопасности), что должно быть обеспечено силами Заказчика.

Прочие требования к защите технических средств, систем связи и передачи данных должны быть уточнены Исполнителем на этапе реализации проекта.

## Требования к защите информации от несанкционированного доступа

В система должны быть реализованы следующие основные механизмы защиты информации от несанкционированного доступа:

* в штатном режиме работы аутентификация администраторов компонентов системы должна осуществляться при помощи службы каталогов Microsoft Active Directory.
* на серверах и рабочих станциях пользователей под управлением ОС Windows, на которых развернуты компоненты системы, должна быть реализована антивирусная защита.
* для информационного обмена между компонентами системы должен использоваться протокол защищенной передачи данных SSL/TLS.

Должен быть выполнен следующий комплекс мер по защите АРМ администраторов системы:

* исключение несанкционированной установки или реконфигурации системного, прикладного ПО и сетевой политики АРМ пользователей Системы;
* идентификация и аутентификация пользователя при входе в операционную систему;
* антивирусная защита АРМ пользователей и администраторов Системы;
* периодическое обновление операционной системы;
* ведение системного журнала аудита по основным событиям информационной безопасности;
* для исключения несанкционированного использования внешних носителей информации (магнитных и оптических дисков, карт памяти, фотоаппаратов, мобильных телефонов), а также произвольных коммуникационных устройств пользователь не должен обладать правами локального администратора на АРМ, должны быть ограничены возможности бесконтрольного подключения магнитных и оптических дисков, карт памяти, фотоаппаратов, мобильных телефонов.

Реализация вышеперечисленных требований по защите АРМ прорабатывается Исполнителем, обеспечивается силами Заказчика.

## Требования к переводу системы в промышленную эксплуатацию

Перед сдачей в эксплуатацию производится автоматизированный и/или ручной анализ для оценки уровня защищенности Системы. Анализ защищенности проводится силами Заказчика.

В случае обнаружения критических с точки зрения ИБ недостатков или уязвимостей сдача Системы в эксплуатацию откладывается до момента устранения замечаний.

При переводе системы в промышленную эксплуатацию должны быть выполнены следующие требования:

* у Исполнителя должны быть изъяты привилегированные полномочия на продуктивном ландшафте системы, как на уровне ОС, так и на прикладном уровне;
* предоставление привилегированных полномочий должно осуществляться только для персонала, обеспечивающего бесперебойное функционирование системы;
* привилегированные полномочия на уровне операционной системы предоставляются персоналу, осуществляющему администрирование информационной системы только в случае, если без данных полномочий невозможно обеспечить бесперебойное функционирование информационной системы;
* при сдаче системы список привилегированных групп направляется в адрес УИБ, для постановки на мониторинг, с указанием ответственного за каждую группу доступа.

## ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ПУСКО-НАЛАДОЧНЫХ РАБОТ

Пуско-наладочные работы выполняются Исполнителем при содействии специалистов Заказчика.

При необходимости изменения настроек существующих компонентов инфраструктуры и информационных систем Заказчика, такие изменения планируются и прорабатываются Исполнителем, согласуются с Заказчиком, выполняются силами Заказчика.

Заказчик определяет и уведомляет Исполнителя о возможных технологических временных «окнах» для проведения работ, требующих выполнения Исполнителем действий, затрагивающих инфраструктуру Заказчика, находящуюся в промышленной эксплуатации.

По запросу Исполнителя Заказчик создаёт в своих информационных системах и приложениях учётные записи, необходимые Исполнителю для выполнения работ в соответствии с согласованной проектной документацией.

Прочие требования к организации пусконаладочных работ должны быть уточнены Исполнителем на этапе реализации проекта.

## ТРЕБОВАНИЯ К ПОРЯДКУ КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ

## Состав и содержание работ

В рамках проекта, после завершения работ, Исполнителем, в зависимости от выбранного решения по реализации, должны быть (созданы, перенесены, развернуты, настроены), все среды системы и подсистем.

При подготовке к вводу в эксплуатацию системы Исполнителю необходимо:

* Обеспечить подготовку полного пакета документов;
* Совместно с Заказчиком определить подразделение и должностных лиц, ответственных за сопровождение и проведение опытной эксплуатации системы;
* Обеспечить обучение пользователей Заказчика работе с системой (в зоне ответственности Исполнителя).

Детальные требования к составу и содержанию работ по подготовке к вводу системы в действие, включая перечень основных мероприятий и их исполнителей должны быть уточнены Исполнителем на начальных этапах проекта.

## Требования к контролю и приемке системы

В целом порядок ввода в эксплуатацию, проведение предварительных и приемочных испытаний системы должны осуществляться в соответствии с требованиями Заказчика.

Объем и последовательность проведения испытаний (предварительных, приемочных) для каждого этапа системы должны быть согласованы с Заказчиком. К проведению испытаний Исполнителем должна быть подготовлена Тестовая модель и сценарии тестирования. Испытания в части выполнения требований ИБ выполняются в продуктивном ландшафте системы. Порядок приемки системы описан далее в настоящем разделе.

Основные требования к документу приведены в Приложении А. Прочие требования должны быть уточнены Исполнителем на этапе проектирования и планирования системы.

## Проведение предварительных испытаний

Предварительные испытания проводятся с целью определения готовности системы к вводу в опытную эксплуатацию.

В ходе предварительных испытаний оценивается соответствие системы требованиям ФТТ и ее работоспособность.

Для проведения предварительных испытаний, Исполнителем, должна быть подготовлена Тестовая модель и сценарии тестирования, утверждаемая Заказчиком.

Результаты предварительных испытаний должны оформляться Исполнителем, тестовыми протоколами по результатам испытаний.

Предварительные испытания системы должны производиться на территории Заказчика.

Прочие требования, должны быть уточнены Исполнителем на этапе проектирования и планирования системы.

## Проведение опытной эксплуатации

Опытная эксплуатация должна проводиться (по утвержденным Заказчиком программам и сценариям) персоналом Заказчика, прошедшим необходимую подготовку, при техническом сопровождении Исполнителя.

В случае наличия отрицательных выводов и заключений по результатам опытной эксплуатации, Исполнителем, должна быть проведена доработка системы по указанным в протоколе пунктам.

Порядок проведения опытной эксплуатации должен быть уточнен на этапе проектирования и планирования системы.

## Требования к поддержке в рамках опытной эксплуатации

 Исполнитель должен обеспечить сопровождение опытной эксплуатации системы с момента сдачи системы в опытную эксплуатацию.

В течение опытной эксплуатации системы сотрудники Исполнителя должны оказывать услуги второй линии поддержки, отвечая на вопросы первой линии поддержки (сотрудников ИТ-подразделения Заказчика), исправлять функционал, если он реализован вне соответствия с ФТТ, проектным решением.

В процессе опытной эксплуатации системы, Заказчиком ведутся журналы обращений пользователей, в которых фиксируются замечания по работе системы и предложения по изменению работы программного обеспечения.

Прочие требования, должны быть уточнены Исполнителем на этапе проектирования и планирования системы.

## Проведение приемочных испытаний

По результатам опытной эксплуатации системы, Исполнителем, должны быть проведены по согласованию с Заказчиком приемочные испытания.

Приемочные испытания должны проводиться согласно тестовой модели и сценариям тестирования на соответствие требованиям ФТТ, а также включать проверку устранения недостатков, выявленных в ходе опытной эксплуатации системы.

Для проведения приемочных испытаний Заказчиком по инициативе Исполнителя должна быть сформирована приемочная комиссия по сдаче системы в промышленную эксплуатацию, которая должна формироваться из специалистов Заказчика и Исполнителя.

По результатам проведения приемочных испытаний Исполнителем должен быть подготовлен Акт о вводе системы в промышленную эксплуатацию.

Прочие требования, должны быть уточнены Исполнителем на этапе проектирования и планирования системы.

## ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ РАБОТ

Ожидаемыми результатами реализации проекта являются:

1. Развернута система класса WAF.
2. Система интегрирована со всеми системами, указанными в разделе 3.4.2.
3. Проведено обучение пользователей и администраторов системы.
4. Целевое количество информационных систем и ресурсов защищены WAF системой.

В результате выполнения работ по проекту должны быть достигнуты целевые показатели, перечисленные в таблице 9.

Таблица 9 - Целевые показатели эффективности проекта

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **п.п.** | **Наименование показателя** | **Базовое значение показателя** | **Целевое значение показателя** | **Отклонение** | **Дата контроля** |
| 1 | Количество опубликованных через новую WAF систему веб-приложений | 0 | 110 | 10% | 30.06.2025 |

Для каждого веб-приложения защищаемого WAF должен быть разработан и согласован с Заказчиком персональный профиль веб-защиты, обеспечивающий безопасность ресурсов.

Прочие требования к результатам работ должны быть уточнены Исполнителем на этапе проектирования и планирования системы.

## ТРЕБОВАНИЯ К ГАРАНТИЙНОМУ ОБСЛУЖИВАНИЮ

Исполнитель должен гарантировать, что результаты оказанных Услуг, предоставленные Заказчику в рамках исполнения настоящих ФТТ, будут соответствовать требованиям, определенным в настоящих ФТТ. Срок гарантийного сопровождения составляет 12 (Двенадцать) месяцев с даты подписания последнего Акта сдачи-приёмки оказанных Услуг по Договору без замечаний со стороны Заказчика.

## ТРЕБОВАНИЯ К ОБУЧЕНИЮ ПЕРСОНАЛА

В рамках реализации проекта Руководитель проекта / Менеджер услуги должен определить потребность в обучении и методологию, организовать подготовку и проведение обучения, оценить эффективность обучения.

В рамках реализации проекта Исполнитель должен подготовить и согласовать с Заказчиком обучающие материалы.

Подход к обучению на проекте описан в таблице 10.

Таблица 10 - Подход к обучению на проекте

|  |  |
| --- | --- |
| 1. | Объем обучения: не более 15 сотрудников Заказчика (5 администраторов, 10 аналитиков) |
| 2. | Уровень сложности функционала: высокий |
| 3. | Модель обучения: одноуровневое обучение на запуске |
| 4. | Формат обучения: очное/дистанционное для аналитиков (специалистов реагирования), администраторов (ответственных экспертов по направлению и непосредственных ответственных за эксплуатацию системы) и поддержки. Для сменных специалистов (аналитиков) должен быть предусмотрен заочный формат с возможностью обучения в группах (для разных смен). Обучение по возможности должно быть основано на ролевой модели Системы. |
| 5. | Инструменты обучения: демонстрация, бизнес-симуляция (администраторы), пользовательский контент |
| 6. | Инфраструктура, среда обучения: Skype/Zoom, учебная песочница/демоверсия, Websoft/видеокурс |
| 7. | Способы и инструменты оценки эффективности обучения: опросы готовности и удовлетворенности пользователей |
| 8. | Перечень обучающих материалов: пошаговая инструкция со скриншотами для КнП, инструкция и видеокурс для администраторов |
| 9. | Ответственные за подготовку и проведение обучения: РП/менеджер услуги; Ответственный за учебные материалы: Исполнитель (подрядчик) |
| 10. | Обучение должно быть организовано с привлечением производителя Системы и получением по завершении обучения соответствующего сертификата. |

## ТРЕБОВАНИЯ К ИНФОРМИРОВАНИЮ И КОММУНИКАЦИИ

В рамках реализации проекта Исполнителем/Заказчиком (менеджер по коммуникациям/менеджер по УИ/РП). должны быть предусмотрены информирование и коммуникации на всем протяжении проекта для обеспечения необходимого уровня осведомленности всех сторон, затронутых трансформацией. Все коммуникации должны быть согласованы с Заказчиком (менеджер по коммуникациям/менеджер по УИ/РП).

В рамках реализации проекта должны быть выпущены ключевые коммуникации, описанные в таблице 11.

Таблица 11 - Ключевые коммуникации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| п.п. | Коммуникация | ЦА | Канал коммуникации | Дата |
| 1 | Создание страницы со всей информацией по проекту (цели, задачи, документы и т.д.) | команда проекта | Confluence | после старта проекта |
| 2 | Статусы по проекту | команда проекта | Skype/Zoom | на регулярной основе |
| 3 | Опрос готовности пользователей к работе по-новому | эксплуатационный персонал | анкетолог или другой сервис | перед выходом в ОПЭ |
| 4 | Информационная рассылка о выходе в ОПЭ | все пользователи | Outlook | выход в ОПЭ |

Прочие требования к информированию и коммуникациям должны быть уточнены Исполнителем/Заказчиком (менеджер по коммуникациям/менеджер по УИ/РП) на этапе проектирования системы и согласованы с Заказчиком (менеджер по коммуникациям/менеджер по УИ/РП).

## ТРЕБОВАНИЯ К ПАТЕНТНОЙ ЧИСТОТЕ

При реализации Системы должно применяться только лицензионное программное обеспечение.

Права на программное обеспечение и систему должны быть переданы Заказчику, за исключением прав на программное обеспечение, предоставление которых регулируется отдельным лицензионным соглашением с правообладателем (разработчиком ПО).

Прочие требования должны быть уточнены Исполнителем на этапе реализации проекта.

## ТРЕБОВАНИЕ К ТЕХНИЧЕСКОЙ ПОДДЕРЖКЕ

После перевода Системы в Промышленную эксплуатацию, Вендором должна оказываться услуга технической поддержки промышленной эксплуатации Системы и Программно-аппаратного комплекса Системы в течение пяти лет.

Услуги технической поддержки должны включать:

* Прием обращений по базовым каналам (портал, телефон);
* Обновление версий Системы;
* Обновление экспертизы;
* Гарантированное время обработки запросов;
* Проактивная и реактивная поддержка;
* Аудит состояния ПО;
* Выполнение работ на площадке Заказчика (при необходимости);
* Выделенный менеджер и канал поддержки;
* Поддержка должна осуществляться 24 часа 7 дней в неделю вне зависимости от производственного календаря.

## Требования к реактивной технической поддержке

Реактивная поддержка предназначена для восстановления работоспособности ландшафтов Системы в случаях отказов и сбоев.

К реактивной поддержке предъявляются требования, описанные в Таблица 12.

Таблица 12 - Требования к реактивной технической поддержке

| Приоритет обращения(инцидента) | Характеристики | Время реакции \*не более, ч. | Время решения \*\*не более, сутки. |
| --- | --- | --- | --- |
| Очень высокий (критичный) | Полная неработоспособность Системы | 1 | 1 |
| Высокий | Система работает в аварийном режиме.  Система не выполняет одну из основных функций.  Система выполняет свои функции при отказе отдельных компонентов.  Система выполняет свои функции при отказе одного «плеча» кластера.  Утилизация аппаратных компонентов Системы критичная. | 2 | 2 |
| Средний | Система работает в штатном режиме.  Есть известные проблемы, которые могут быть причиной инцидента высокого приоритета. | 6 | 6 |
| Низкий | Система работает в штатном режиме.  Прочие ошибки и проблемы, не влияющие существенно на функции и работоспособность Системы | 12 | 12 |

\* Время реакции – время от момента создания заявки Заказчиком до получения Заказчиком подтверждения от Исполнителя, что его заявка принята к обслуживанию.

\*\* Время решения – время от момента создания заявки Заказчиком до любого из вариантов:

* момента подтверждения Заказчиком, что заявка выполнена (проблема решена);
* момента подтверждения Заказчиком, что приоритет заявки понижается;
* момента подтверждения Заказчиком, что дальнейшие действия по устранению проблемы находятся в зоне ответственности Заказчика.

Для продуктивных сред системы приём и обработка заявок должны осуществляться круглосуточно.

Прочие требования к реактивной поддержке должны быть определены Исполнителем и согласованы с Заказчиком, на фазе проектирования и планирования системы.

## Требование к проактивной технической поддержке

Проактивная поддержка должна включать в себя профилактические мероприятия, направленные на оптимизацию работы, непрерывное улучшение процессов управления и эксплуатации Системы.

Проактивная поддержка должна состоять из работ по обеспечению:

* Жизнедеятельности систем: мониторинг состояния доступности и производительности систем и их компонентов, входящих в объем проекта с последующим анализом и оптимизацией параметров систем, либо выполнением требуемых работ (при необходимости), для повышения уровня производительности и надежности;
* Мониторинга и оптимизации работы системы и баз данных;
* Мониторинга и оптимизации использования аппаратных ресурсов;
* Мониторинга и оптимизации заданий резервного копирования компонентов системы;
* Мониторинг дампов, процессов обновления системы;
* Консультаций специалистов Заказчика по эксплуатационным вопросам.

Прочие требования к проактивной поддержке должны быть уточнены Исполнителем и согласованы с Заказчиком, на этапе проектирования и планирования.

## Требование к работам по заявкам

Работы по заявкам должны включать в себя:

* Установка сервис-паков и обновлений по запросу;
* Участие в разборе проблемных ситуаций, возникающих в процессе внедрения и эксплуатации систем, входящих в объем проекта (совместно со специалистами Заказчика);
* Выполнение резервирования восстановления компонентов системы по запросу;
* Подключение пользователей к системе.

Прочие требования, должны быть уточнены Исполнителем и согласованы с Заказчиком, на фазе проектирования и планирования.

## ТРЕБОВАНИЕ К ДОКУМЕНТИРОВАНИЮ

Документирование системы в рамках проектирования и реализации должно производиться в соответствии с требованиями корпоративных стандартов Заказчика в части создания корпоративных информационных систем и порядку их описания/разработки.

Комплект эксплуатационной документации должен быть передан Исполнителем, как на бумажных, так и на машинных носителях в службу эксплуатации Заказчика. (на машинных носителях – в формате документов Microsoft Office 2010 и выше).

Дополнительно для текстовых документов - формат «Adobe Acrobat Document» – «pdf».

Для графических документов - формат «Файлы MS Visio»- «VSDX» и «VSDM».

По согласованию с Заказчиком документирование может выполняться в электронном виде в среде Confluence.

По результатам реализации проекта Исполнитель должен разработать, согласовать, предъявить и передать Заказчику документы, перечисленные в Приложении А.

Каждый документ является неотъемлемой частью процедуры передачи системы на сопровождение. Без передачи всего комплекта проектной документации службе эксплуатации Заказчика проект не может считаться завершенным

## ТРЕБОВАНИЕ К УСЛОВИЯМ ДОГОВОРА

Общая длительность работ по проекту не должна превышать 10 календарных месяцев (200 рабочих дней) с момента подписания договора.

Предварительные сроки предоставления результатов проекта должны соответствовать требованиям, указанным в Приложении Б.

Сроки должны быть уточнены Исполнителем и согласованы Заказчиком на этапе проектирования системы.

Визуальное управление – ведение наглядных ежедневно обновленных панелей, отслеживающих статус выполнения работ и принятия результатов в Jira.

## ЛИСТ СОГЛАСОВАНИЯ

|  |  |  |  |
| --- | --- | --- | --- |
| **п.п.** | **Должность** | **Результат согласования** | **Фамилия, инициалы** |
| 1 | Руководитель направления центра кибербезопасности Управление информационной безопасности | Согласовано 19.09.24 | Телехина И.Г. |
| 2 | Руководитель направления методологии Управление информационной безопасности | Согласовано 20.09.24 | Авдеев Д.К. |
| 3 | Ведущий архитектор решений Направление по развитию ИТ-инфраструктуры, | Согласовано 20.09.24 | Валиахметов Д.А. |
| 4 | Архитектор по ИБ, Руководитель направления, Группа архитектуры ИБ | Согласовано 25.09.24 | Конюхов А.Н. |
| 5 | Руководитель направления по сетевым технологиям | Согласовано 24.09.24 | Литвинов И.М. |
| 6 | Начальник управления Дирекция по инфраструктуре и информационной безопасности | Согласовано 26.09.24 | Овчинников А.Г. |

## ПРИЛОЖЕНИЕ А

Требования к содержанию эксплуатационной документации

|  |  |  |
| --- | --- | --- |
| Наименование документа | Тип документации | Требования к содержанию |
| Проектное решение | Технический проект | Документ должен описывать полный ландшафт технической инфраструктуры. Содержать детальные схемы, их описания, настройки для каждого компонента системы, описывать информационные потоки между системами и подсистемами, содержать детальные требования к межсетевому взаимодействию, и т.д. Описывать подходы к мониторингу, резервному копированию, обслуживанию системы. Описывать процедуры обеспечения отказоустойчивости, высокой доступности (если используется) и т.д.  В состав документа должны быть включены:   * Пояснительная записка к техническому проекту (Техническое решение); * Общая, логическая, сетевая схемы; * Схема функциональной структуры; * Компоненты системы; * Схема и таблицы сетевых взаимодействий; * Схема балансировки и публикации в интернет; * Интеграционные взаимодействия; * Технологические/сервисные учетные записи; * Реестр ролей и полномочий, Описание доступа к системе; * Сайзинг комплекса технических средств и спецификация оборудования (документ должен описывать требования, предъявляемые к системе и к функционированию системы, входные условия оценки и описания расчетов по каждому элементу комплекса технических средств). |
| Скрипты и регламент резервного копирования | Эксплуатационная документация | Описание процедур резервного копирования Системы |
| Скрипты и регламент аварийного восстановления системы | Эксплуатационная документация | Описание процедур восстановления Системы |
| Скрипты и регламент обслуживания системы | Эксплуатационная документация | Описание процедур обслуживания Системы |
| Инструкция по реагированию на инциденты ИБ | Эксплуатационная документация | Инструкция администраторов и пользователей по реагированию на инциденты ИБ |
| Регламент тестирования и установки обновлений | Эксплуатационная документация | Описание процедур тестирования и обновления Системы |
| Регламент масштабирования | Эксплуатационная документация | Описание правил и процедуры масштабирования Системы |
| Регламент мониторинга | Эксплуатационная документация | Описание процедур мониторинга Системы |
| Регламент аварийного восстановления | Эксплуатационная документация | Описание процедур аварийного восстановления Системы |
| Пользовательские материалы (руководства пользователей системы, регламент проведения работ по обслуживанию, регламент резервного копирования инструкции, памятки и др. обучающие материалы) | Эксплуатационная документация | Документ должен описывать порядок действий пользователя в ИТ-системе для выполнения функций соответствующей его роли, содержать описание функций, транзакции, шаги, системные экраны и правила заполнения. |
| Инструкция администратора системы | Эксплуатационная документация | Документ должен описывать функции, транзакции, шаги, системные экраны, правила заполнения и т.д. Включать требования к плану восстановления системы, работам по обслуживанию и обновлению. |
| Программа и методики предварительных испытаний  Программа и методики опытной эксплуатации;  Протокол предварительных испытаний Системы | Рабочая документация | Описание программы и методики предварительных испытаний и результаты испытаний, отображенные в протоколе. В протоколе должны быть отражены результаты проведенных проверок по каждому пункту программы, выводы и рекомендации по ним. |
| Акт о готовности Системы к переводу в промышленную эксплуатацию | Рабочая документация | В протоколе должны быть отражены результаты проведенных проверок по каждому пункту программы, выводы и рекомендации по ним. |
| Журнал опытной эксплуатации | Рабочая документация | Замечания к Системе и пожелания Заказчика должны быть зафиксированы и учтены в журнале опытной эксплуатации. |
| Программа и методика приемочных испытаний | Рабочая документация | Описание программы и методики приемочных испытаний и результаты испытаний, отображенные в протоколе. Должны быть учтены и исправлены замечания по результатам опытной эксплуатации. |
| Протокол приемо-сдаточных испытаний Системы | Рабочая документация | В протоколе должны быть отражены результаты проведенных проверок по каждому пункту программы, выводы и рекомендации по ним. |
| Акт о готовности информационной системы к переводу в промышленную эксплуатацию | Рабочая документация | Документ должен содержать подтверждение готовности приемки системы\модуля\функциональности на поддержку |

## ПРИЛОЖЕНИЕ Б

**Календарный План-график реализации проекта внедрения  
Системы защиты web-приложений (WAF)**

| **№** | **Состав работ** | **Дата начала** | **Дата окончания** | **Кол-во раб. дней** | **Ответственный** | **Стоимость, тыс. руб., в т.ч. НДС** |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Подготовительные работы** |  |  |  |  |  |
|  | Создание проектной команды Исполнителя и Заказчика |  |  |  | Заказчик, Исполнитель |  |
|  | Kick-off митинг |  |  |  | Заказчик, Исполнитель |  |
|  | Проведение обследования существующей Системы WAF, ИТ-инфраструктуры и процессов публикации веб-приложений и веб-ресурсов |  |  |  | Исполнитель |  |
|  | Разработка lетального плана проекта |  |  |  | Исполнитель |  |
|  | Подготовка и согласование сайзинга (требований к развертыванию ПАК на продуктовой среде) |  |  |  | Исполнитель |  |
|  | Выдача рекомендаций по предварительным настройкам инфраструктуры |  |  |  | Исполнитель |  |
|  | Закупочные процедуры Заказчика (ПАК, ИТ-инфраструктура, при необходимости) |  |  |  | Заказчик |  |
|  | Пуско-наладка ПАК ИТ-инфраструктуры Заказчика (конфигурирование ПАК, при необходимости) |  |  |  | Заказчик |  |
|  | Подписание акта сдачи-приемки работ |  |  |  | Заказчик, Исполнитель |  |
|  | **Проектная документация** |  |  |  |  |  |
|  | Разработка и согласование проектной документации в соответствии с Приложением А «Требования к содержанию проектной и эксплуатационной документации» (предоставить детальный уточненный план разработки и согласования) |  |  |  | Заказчик, Исполнитель |  |
|  | Подписание акта сдачи-приемки работ. |  |  |  | Заказчик, Исполнитель |  |
|  | **Развертывание и настройка Системы WAF** |  |  |  |  |  |
|  | Развертывание Системы WAF и её базовая настройка |  |  |  | Исполнитель |  |
|  | Настройка правил защиты веб-приложений (до 110 шт.): индивидуального профиля, определяющего правила обработки запросов и ответов между браузером пользователя и приложением. Определение и настройка механизмов защиты. |  |  |  | Исполнитель |  |
|  | Настройка действий и реагирования на события в случае обнаружения атаки: уведомление, блокировка, запись в журнал |  |  |  | Исполнитель |  |
|  | Определение и настройка правил и адресатов для уведомлений об обнаруженных атаках и событиях |  |  |  | Исполнитель |  |
|  | Мониторинг и внесение изменений в политики для исключения ложноположительных срабатываний |  |  |  | Исполнитель |  |
|  | Перевод системы в блокирующий режим |  |  |  | Исполнитель |  |
|  | Настройка интеграций с системами ИБ (SIEM, SOAR) |  |  |  | Исполнитель |  |
|  | Проведение тестовых испытаний Системы WAF |  |  |  | Заказчик, Исполнитель |  |
|  | Соответствие требованиям ТП |  |  |  | Заказчик, Исполнитель |  |
|  | Соответствие требованиям ИБ |  |  |  |  |
|  | DRP тест |  |  |  |  |
|  | Подписание акта сдачи-приемки работ |  |  |  | Заказчик, Исполнитель |  |
|  | **Эксплуатационная документация** |  |  |  | Исполнитель |  |
|  | Разработка и согласование эксплуатационной документации в соответствии с Приложением А «Требования к содержанию проектной и эксплуатационной документации» (предоставить детальный уточненный план разработки и согласования) |  |  |  | Заказчик, Исполнитель |  |
|  | Подписание акта сдачи-приемки работ. |  |  |  | Заказчик, Исполнитель |  |
|  | **Опытно-промышленная эксплуатация**  **Системы WAF** |  |  |  |  |  |
|  | Обучение администраторов и ключевых пользователей (аналитиков) Системы WAF |  |  |  | Заказчик, Исполнитель |  |
|  | Проведение ОПЭ Системы WAF |  |  | 20 | Заказчик, Исполнитель |  |
|  | Доработка документации по итогам опытной эксплуатации |  |  |  | Исполнитель |  |
|  | Приёмо-сдаточные испытания,  Протокол проведения ОПЭ Системы WAF с реестром замечаний и отметками об их устранении |  |  |  | Заказчик, Исполнитель |  |
|  | Подписание акта сдачи-приемки работ. |  |  |  | Заказчик, Исполнитель |  |
|  | **Подписание Акта о готовности Системы WAF к вводу в ПЭ** |  |  |  | Заказчик, Исполнитель |  |
| **Итого:** | |  |  | **до 200** |  | **ХХХ** |

## ПРИЛОЖЕНИЕ В

Регламент резервного копирования

Регламент РК.doc