

Утверждено:

Начальник Управления по информационной безопасности ООО «ЭН+ГИДРО»



А.А. Афанасьев

(подпись)

« 18 » 06 2026 г.

Техническое задание

Система анализа безопасности приложений

ОГЛАВЛЕНИЕ

ТЕРМИНЫ И СОКРАЩЕНИЯ	3
1. ОБЩИЕ СВЕДЕНИЯ	4
2. ГРАНИЦЫ ПРОЕКТА.....	5
3.ЦЕЛИ И ЗАДАЧИ СОЗДАНИЯ СИСТЕМЫ.....	6
3.1. Цели создания Системы.....	6
3.2. Задачи Системы.....	6
4. ТРЕБОВАНИЯ К АРХИТЕКТУРЕ СИСТЕМЫ	7
5. ФУНКЦИОНАЛЬНЫЕ ТРЕБОВАНИЯ К СИСТЕМЕ	8
5.1.Общие требования к Системе.....	8
5.2.Требования к функциям, выполняемым Системой	8
5.3. Требования к отчетности Системы.....	10
6. ТРЕБОВАНИЯ К ИТ-ИНФРАСТРУКТУРЕ.....	11
6.1 Требования к техническому обеспечению	11
6.2. Требования к доступности.....	11
6.3. Требования к диагностированию системы.....	11
6.4. Требования к масштабированию Системы.....	11
6.5. Требования к надежности Системы	11
6.7. Требования к интеграции с инфраструктурными сервисами.....	12
6.8. Требования к программному обеспечению.....	12
6.9. Требования к техническим средствам.....	12
6.10. Требования к энергоэффективности	12
6.11. Требования к поставке материалов, оборудования и программного обеспечения	13
6.12. Требования к рабочим местам пользователей Системы.....	13
7. ТРЕБОВАНИЯ К ИБ.....	14
7.1. Требования к техническому решению на обеспечение ИБ Системы.....	14
7.2. Регистрация значимых событий ИБ.....	14
7.3. Обеспечение целостности программной среды	14
7.4. Требования к защите информации от несанкционированного доступа.....	14
7.5. Требования к резервному копированию.....	15
8. ТРЕБОВАНИЯ К УПРАВЛЕНИЮ ПРОЕКТОМ	16
9. ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ПУСКОНАЛАДОЧНЫХ РАБОТ	17
10. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ РАБОТ	18
11. ТРЕБОВАНИЯ К ГАРАНТИЙНОМУ ОБСЛУЖИВАНИЮ.....	19

12. ТРЕБОВАНИЯ К ЧИСЛЕННОСТИ И КВАЛИФИКАЦИИ ПЕРСОНАЛА, ОБСЛУЖИВАЮЩЕГО СИСТЕМУ, И РЕЖИМУ ЕГО РАБОТЫ.....	21
13. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ	22
13.1. Требования к составу эксплуатационной документации	22
13.2. Требования к оформлению документации.....	22

Термины и сокращения

В настоящем документе использованы следующие термины и сокращения:

Обозначение	Описание
АРМ	автоматизированное рабочее место
ГОСТ	государственный стандарт
ИБ	информационная безопасность
ИТ	информационные технологии
ИС	инструментальное средство
ПКБПО, Система	программный комплекс контроля безопасности программного обеспечения
НДВ	недекларированные возможности
НТД	нормативно-техническая документация
ОС	операционная система
ПО	программное обеспечение
ПК	программный комплекс
СЗИ	средства защиты информации
API	(англ. application programming interface), программный интерфейс приложения
CI/CD	(англ. continuous integration/continuous delivery) комбинация непрерывной интеграции и непрерывного развертывания ПО в процессе разработки
Git	распределенная система управления версиями
GitLab	инструмент для хранения и управления репозиториями Git
Gitlab CI	инструмент, встроенный в GitLab для автоматизации задач, которые возникают в процессе разработки программного обеспечения
Jenkins	программная система с открытым исходным кодом на Java, предназначенная для обеспечения процесса непрерывной интеграции программного обеспечения
SBOM	формат файла с описанием используемых компонентов
SVN	свободная централизованная система управления версиями

1. Общие сведения

Полное наименование системы: Программный комплекс контроля безопасности программного обеспечения в корпоративной информационной системе (далее – Система)

Сокращенное наименование системы: ПККБПО

Исполнитель: (далее – Исполнитель) определяется по результатам открытого конкурса.

Заказчик: ООО «ЭН+ ГИДРО» (далее – Заказчик).

2. Границы проекта

Плановые сроки начала и окончания работы по созданию Системы:

- плановый срок начала работ – с даты заключения договора;
- плановый срок окончания работ – 20 рабочих дней с даты заключения договора.

3. Цели и задачи создания Системы

3.1. Цели создания Системы

Система создается с целью:

- разработки и внедрения механизмов контроля передачи программного обеспечения Заказчику;
- повышения контроля за разработкой программного обеспечения в интересах Заказчика;
- приведение процесса разработки программного обеспечения в соответствие требованиям регуляторов.

3.2. Задачи Системы

Система должна:

- обеспечивать анализ приложений на возможные уязвимости ИБ и НДС используемого Заказчиком ПО;
- соответствовать требованиям регуляторов в области защиты информации;
- сокращать затраты на устранение уязвимостей, обнаруженных на поздней стадии уже в работающем приложении, а также предупреждать клиентские потери вследствие компрометации или сбоя в работе приложений;
- снижать риски сбоев в работе приложений и простоев систем вследствие проблем безопасности.

4. Требования к архитектуре Системы

Архитектура ИС должна обеспечивать быстродействие и отказоустойчивость Системы. Взаимодействие с пользователем, распределение задач и анализ кода выполняется отдельными модулями. Кроме того, в зависимости от потребностей пользователя в установку могут быть включены / не включены модули для анализа приложений на разных языках программирования и динамического анализа безопасности приложений.

Система должна состоять из следующих подсистем:

- подсистема статического анализа;
- подсистема динамического анализа;
- подсистема анализа сторонних компонентов;
- подсистема анализа цепочки поставок;
- подсистема анализа лицензионных рисков;
- подсистема отчетности.

5. Функциональные требования к Системе

5.1. Общие требования к Системе

В составе ИС должны быть следующие функции:

- анализ программного обеспечения на соответствие требованиям ИБ по исходному коду;
- анализ программного обеспечения на соответствие требованиям ИБ по byte-коду (методом статического анализа) при отсутствии debug info и исходных кодов;
- анализ программного обеспечения на соответствие требованиям ИБ методом динамического анализа;
- поиск НДВ в ПО;
- поиск уязвимых сторонних компонентов;
- анализ цепочки поставок ПО;
- анализ лицензионных рисков;
- генерация оценки доверия для используемых сторонних компонентов;
- по результатам анализа приложений ИС должно выдавать рекомендации по настройке средств защиты информации для таких уязвимостей и НДВ, эксплуатация которых может быть предотвращена при помощи настройки СЗИ.

Поиск уязвимостей и НДВ должен осуществляться при помощи следующих методов статического анализа:

- анализ по шаблонам;
- анализ потока управления
- taint-анализ;
- анализ синонимов;
- анализ распространения констант;
- анализ распространения типов;

5.2. Требования к функциям, выполняемым Системой

5.2.1. Требования к анализу ПО по исходному коду

Анализ ПО по исходному коду должен удовлетворять следующим требованиям:

- ИС должно выполнять анализ исходного кода на языках Java, Java for Android, JavaScript, JSP, TypeScript, VBScript, Scala, HTML5, PHP, Python, Groovy, Kotlin, Go, Ruby, C#, C/C++, Objective-C, Swift, ABAP, Apex, Solidity, PL/SQL, T/SQL, Visual Basic 6.0, Delphi, COBOL, VBA, 1C, ASP.NET, Perl, Vyper, VB.NET, LotusScript, Pascal, Dart, Rust;
- ИС должно транслировать исходный код во внутреннее представление;
- ИС должно обеспечивать интеграцию со средствами сборки;
- ИС должно обеспечивать корреляцию результатов с динамическим методом анализа, если такой проводился для данного приложения;

- для полученного внутреннего представления должны применяться методы поиска уязвимостей и НДВ, описанные в п. 5.1.

5.2.2. Требования к анализу ПО по byte-коду

Анализ ПО по byte-коду должен удовлетворять следующим требованиям:

- ИС должно выполнять анализ byte-кода, полученного посредством трансляции из языков: Java/Scala: JAR/WAR/EAR/AAR; C/C++: DLL/EXE; Android: APK; Apple iOS: IPA; Apple macOS: APP;
- ИС должно транслировать byte-код во внутренне представление;
- ИС должно обеспечивать корреляцию результатов с динамическим методом анализа, если такой проводился для данного приложения;
- для полученного внутреннего представления должны применяться методы поиска уязвимостей и НДВ, описанные в п. 5.1.

5.2.3. Требования к анализу ПО методом динамического анализа

Анализ ПО методом динамического анализа должен удовлетворять следующим требованиям:

- ИС должно выполнять анализ работающего приложения (веб-приложения) путем доступа к нему по сети (TCP/IP), по протоколу http (https);
- ИС должно иметь возможность при проверке приложения проводить в нем аутентификацию по средствам логина/пароля, токена, заголовков, форм авторизации при наличии в приложении такой функциональности;
- ИС должно иметь возможность проводить динамический анализ приложения с использованием AJAX-запросов;
- ИС должно иметь возможность исключать из анализа приложения конечные пути проверки, определенные пользователем ИС;
- ИС должно иметь возможность использовать для анализа схему API исследуемого приложения, если данная схема может быть представлена в виде отдельного компонента на выделенном URL;
- ИС должно иметь возможность выбирать режим сканирования.

5.2.4. Требования к анализу ПО методом анализа сторонних компонентов

Анализ ПО методом анализа сторонних компонентов должен удовлетворять следующим требованиям:

- ИС должно выполнять анализ сторонних компонентов на известные уязвимости (CVE) по архиву с исходным кодом;
- ИС должно выполнять анализ сторонних компонентов на известные уязвимости (CVE) по SBOM-файлу;
- ИС должно выполнять анализ цепочки зависимостей на безопасность уязвимости по SBOM-файлу;
- ИС должно проверять лицензионную чистоту сторонних компонентов по SBOM-файлу.

5.3. Требования к отчетности Системы

ИС должно предоставлять отчетность по результатам анализа приложения, соответствующую следующим требованиям:

- вся отчетность должна предоставляться на русском и английском языках;
- отчет должен удовлетворять специфичным требованиям для различных категорий пользователей;
- отчет должен предоставляться в различных формах в зависимости от метода проведенного сканирования (после динамического, статического анализа или анализа состава ПО);
- для разработчиков отчет должен содержать прогресс изменения состояния безопасности разрабатываемого кода;
- для офицеров ИБ отчет должен содержать метрики, позволяющие сравнить анализируемое приложение со средним по отрасли;
- для руководителей отчет должен содержать прогресс работы над проектом в целом;
- администраторы и пользователи должны иметь возможность настраивать информацию, выгружаемую в отчет: выбирать приложения, выбирать категории уязвимостей.

6. Требования к ИТ-инфраструктуре

6.1. Требования к техническому обеспечению

Технические средства, необходимые для создания Системы, должны соответствовать рекомендуемым требованиям производителей программных и аппаратных средств.

Аппаратные платформы для серверов Системы должны соответствовать следующим требованиям:

Требование	Описание
Кол-во процессоров	не менее 2
Объем оперативной памяти	не менее 64 ГБ
Объем памяти НЖМД	не менее 600 ГБ
Кол-во блоков питания	не менее 2
Кол-во сетевых интерфейсов	не менее 2

6.2. Требования к доступности

Система должна поддерживать работу в круглосуточном режиме (24x7x365) с запланированными перерывами на технологическое обслуживание.

Система должна обеспечивать модульность и интегрируемость – возможность использования компонентов Системы совместно или независимо друг от друга.

Любое из аппаратных средств Системы должно допускать замену его средством с аналогичными функциональными и техническими характеристиками без каких-либо конструктивных изменений или регулировки в остальных технических средствах Системы (кроме случаев, специально оговоренных в технической документации на компоненты Системы).

6.3. Требования к диагностированию системы

Система должна логировать действия, совершенные пользователями, в соответствующие журналы событий.

Ошибки при работе пользователя с Системой должны выводиться в веб-интерфейс и содержать информацию об ошибке, которая поможет ее исправить.

6.4. Требования к масштабированию Системы

Архитектура ИС должна обеспечивать взаимодействие с пользователем, распределение задач и анализ кода должны выполняться отдельными модулями. Кроме того, в зависимости от потребностей Заказчика в установку могут быть включены / не включены модули для анализа приложений на разных языках программирования, динамического анализа приложений и анализа состава ПО.

6.5. Требования к надежности Системы

Уровень надежности Системы зависит от основных факторов:

- надежности и отказоустойчивости используемых технических средств в составе технической инфраструктуры (серверное оборудование, сетевое оборудование, рабочие станции пользователей);
- надежности функционирования прикладного программного обеспечения;
- квалификации персонала, администрирующего и обслуживающего Систему;
- качества планирования и организации работ по сопровождению Системы;
- компоненты используемого прикладного ПО не должны нарушать целостности друг друга;
- интегрируемые с системой внешние системы должны функционировать в штатном режиме.

6.6. Требования к интеграции с инфраструктурными сервисами

ИС необходима возможность по интеграции с репозиториями SVN/Git. Сервисами CI/CD Jenkins, TeamCity, Azure DevOps Server, Gitlab CI. VCS хостингами GitHub, GitLab, BitBucket. Средствами отслеживания ошибок Jira. С помощью открытого встроенного API должна быть доступна интеграция с другими системами и сервисами.

6.7. Требования к программному обеспечению

Все программные средства, необходимые для создания Системы, а также лицензии на их использование должны быть приобретены и оформлены в соответствии с лицензионными соглашениями, предлагаемыми производителями.

6.8. Требования к техническим средствам

Система должна быть рассчитана на эксплуатацию в составе ИТ-инфраструктуры Заказчика, соответствовать установленным нормам и правилам Заказчика, а также рекомендациям изготовителей ПО и оборудования. Техническая и физическая защита аппаратных компонентов Системы, носителей данных, бесперебойное энергоснабжение, текущее обслуживание реализуются техническими и организационными средствами, имеющимися у Заказчика.

Регламентные работы по обслуживанию оборудования и программного обеспечения должны проводиться в часы работы Заказчика.

Регламентные работы, ограничивающие работу пользователей ИС, должны проводиться по согласованию с Заказчиком в нерабочее время для подразделений, обрабатывающих документы. При необходимости проведения таких регламентных работ в рабочее время пользователи ИС должны быть заранее (не менее чем за 4 часа) предупреждены.

6.9. Требования к энергоэффективности

Технические средства, необходимые для создания Системы, в части энергоэффективности должны соответствовать рекомендуемым требованиям производителей программных и аппаратных средств.

6.10. Требования к поставке материалов, оборудования и программного обеспечения

В рамках реализации Системы должны быть в установленном у Заказчика порядке разработаны новые или скорректированы действующие корпоративные НТД и регламенты, необходимые для эксплуатации Системы в объеме функционала, предусмотренного настоящим техническим заданием.

6.11. Требования к рабочим местам пользователей Системы

АРМ пользователя Системы должно быть оборудовано персональным компьютером с подключением к внутренней сети компании.

7. Требования к ИБ

7.1. Требования к техническому решению на обеспечение ИБ Системы
ИС должно соответствовать следующим требованиям ИБ:

- контроль доступа пользователей ИС к ресурсам ИС должен осуществляться в соответствии с правами пользователей, настраиваемыми администратором;
- доступ к ресурсам ИС должен осуществляться только при помощи индивидуального логина и пароля;
- пароли пользователей должны храниться в зашифрованном виде;
- доступ к функциям администратора должен происходить только по индивидуальному логину и паролю администратора;
- должно быть обеспечено разделение доступа к функционалу ИС по уровням иерархии;
- если пользователь ИС неактивен в течение некоторого периода времени, в Системе должна быть предусмотрена возможность автоматического выхода из Системы;
- должно осуществляться логирование действий пользователей и администраторов.

7.2. Регистрация значимых событий ИБ

ИС должно предоставлять следующие функциональные возможности в интерфейсе для роли администратора:

- просмотр журналов действий пользователей и работы ИС.

ИС должно предоставлять следующие функциональные возможности в интерфейсе для ролей разработчика, офицера ИБ, руководителя:

- история сканирований.

7.3. Обеспечение целостности программной среды

Система должна обеспечивать модульность и интегрируемость – возможность использования компонентов Системы совместно или независимо друг от друга.

Любое из аппаратных средств Системы должно допускать замену его средством с аналогичными функциональными и техническими характеристиками без каких-либо конструктивных изменений или регулировки в остальных технических средствах Системы (кроме случаев, специально оговоренных в технической документации на компоненты Системы).

7.4. Требования к защите информации от несанкционированного доступа

ИС должно предоставлять следующие функциональные возможности в интерфейсе для роли администратора:

- просмотр списка всех пользователей Системы;
- возможность изменения учетных данных пользователей Системы;

- возможность изменения прав доступа для пользователей Системы;
- возможность настройки журналирования действий пользователей и работы ИС.

7.5. Требования к резервному копированию

Резервное копирование компонентов Системы должно осуществляться в соответствии с регламентами, установленными у Заказчика.

8. Требования к управлению проектом

ИС должно предоставлять следующие функциональные возможности:

- предоставлять всю информацию на русском языке;
- предоставлять единую точку доступа к информации, предоставляемой Системой.

Интерфейс Системы должен быть адаптирован для следующих категорий пользователей:

- администратор;
- сотрудник ИБ;
- разработчик.

9. Требования к организации пусконаладочных работ

Пусконаладочные работы проводятся после обеспечения Заказчиком следующих условий для внедрения:

- предоставление помещения для выполнения работ;
- предоставление инфраструктуры и вычислительных мощностей.

Перед началом пусконаладочных работ Исполнитель должен разработать и согласовать с Заказчиком план пусконаладочных работ. План пусконаладочных работ должен содержать:

- монтаж и настройку оборудования;
- коммутацию сетевого оборудования, настройку сетевого взаимодействия между элементами;
- установку общесистемного ПО;
- установку компонентов Системы согласно проектной документации;
- установку лицензий на компоненты Системы;
- настройку компонентов Системы согласно проектной документации;
- комплексное тестирование компонентов Системы и проведение предварительных испытаний.

10. Требования к результатам работ

Результатом работ должен являться созданный в соответствии с решениями технического проекта комплекс технических и программных средств Системы, готовый к опытной эксплуатации.

11. Требования к гарантийному обслуживанию

Гарантийное обслуживание направлено на устранение неполадок в работе Системы, а также дефектов, препятствующих нормальной эксплуатации программного обеспечения.

Срок, в течение которого действует гарантия на программное обеспечение, предусмотрен в лицензионном договоре.

Исполнитель предоставляет гарантийное обслуживание только в отношении своего программного обеспечения. Гарантийное обслуживание программного обеспечения третьих лиц не осуществляется.

В рамках гарантийного обслуживания программного обеспечения Исполнитель предоставляет:

- возможность размещения запросов на гарантийное обслуживание в автоматизированной системе обработки запросов через диспетчерскую службу, по электронной почте;
- при обработке запроса – возможность расширенной диагностики проблем и выдачу рекомендаций по их устранению (средствами удаленного мониторинга и управления, при условии доступа к этим средствам через интернет);
- результаты решений по запросам, включая:
 - консультации по устранению выявленных инцидентов
 - консультации по телефону и электронной почте по вопросам, связанным с настройками и администрированием Системы
 - заключение о причинах отклонений от корректного поведения Системы, описанного в документации: неправильное использование, ошибка в документации, ошибка в программном обеспечении
 - рекомендации по эксплуатации Системы, если отклонение от корректного поведения вызвано неправильным ее использованием
 - временные решения по дефектам
 - временные решения по выявленным ошибкам, если это возможно
 - оценку срока выпуска версий, в которых будут устранены выявленные ошибки
- обновления и исправления (патчи) Системы, изменения, производимые в рамках текущей версии программного обеспечения в пределах срока гарантийного обслуживания;
- по запросу – новые версии документации продуктов-компонентов.

Ключевые параметры гарантийного обслуживания:

№	Наименование	Значение
1	Режим гарантийного обслуживания (возможность обращения пользователя по гарантийным случаям)	
1.1	Прием запросов по электронной почте	24×7 Ежедневно, круглосуточно
1.2	Прием запросов диспетчерской службой	8×5 По рабочим дням с 9:00 до 17:00 ИРК
1.3	Ответ специалистов	8×5 По рабочим дням с 9:00 до 17:00 ИРК
2	Удаленная диагностика проблем	Предоставляется
3	Время реагирования на запросы согласно уровню критичности	
3.1	ОЧЕНЬ СРОЧНЫЙ Ошибка в работе компонентов программного обеспечения, приводящая к отказу или сбою в функционировании программного обеспечения, способная привести к остановке или снижению производительности бизнес-процессов пользователя и не имеющая никакого временного решения	Не более 4 рабочих часов
3.2	СРОЧНЫЙ Ошибка в работе компонентов программного обеспечения, которая отчасти затрагивает бизнес-процессы пользователя	Не более 8 рабочих часов
3.3	СТАНДАРТНЫЙ Вопросы или ошибки, связанные с работой компонентов программного обеспечения или касающиеся эксплуатационной документации на программное обеспечение (компоненты программного обеспечения), никак не влияющие на бизнес-процессы пользователя, однако относящиеся к категории неполадок работы программного обеспечения	Не позднее следующего рабочего дня

12. Требования к численности и квалификации персонала, обслуживающего Систему, и режиму его работы

К процедуре на выполнение работ по созданию Системы в качестве исполнителей допускаются компании, обладающие следующими квалификацией, опытом и компетенциями:

- Исполнитель должен представить информацию о команде, обладающей опытом внедрения предлагаемого программного продукта, аналогичных решений, находящихся в продуктивной эксплуатации;
- Исполнитель должен предоставить информацию о ранее внедренных системах предлагаемого программного продукта, аналогичных решениях, находящихся в продуктивной эксплуатации с указанием компании-заказчика;

13. Требования к документированию

13.1. Требования к составу эксплуатационной документации

В рамках проекта должна быть разработана следующая документация (список неокончательный и может быть расширен для достижения целей проекта):

- общее описание Системы;
- технические требования к инфраструктуре, на которой будет развернута Система;
- пользовательская документация.

13.2. Требования к оформлению документации

Вся документация, сопровождающая проект и передаваемая Исполнителем Заказчику, должна быть в виде файлов в формате MS Word.