ПРОЕКТ

ТЕХНИЧЕСКОГО ЗАДАНИЯ
на проведение аудита ИТ-инфраструктуры включая информационные системы Агентства по защите депозитов Кыргызской Республики

Бишкек 2022 г.

Информационная безопасность и программно-технологическое обеспечение.

Цели и задачи Агентства в области информационных технологий направлены на его инновационное развитие для совершенствования всех направлений деятельности в части безопасности, сохранности и дальнейшего развития программно-технологического обеспечения.

В Агентстве структура архитектуры IT состоит из комплекса технических средств (КТС), специального и пользовательского программного обеспечений, Интернет, электронной почты, сети передачи данных.

I. Состав комплекса технических средств:

1. Сервер Агентства:
   - Сервер приложений;
   - Сервер баз данных;
   - Ленточный накопитель;
   - Источники бесперебойного питания.
2. Персональные компьютеры (ПК):
   - Стационарные пользовательские ПК – 9 единиц;
   - Переносные ПК – ноутбуки - 8 единиц.
3. Аппаратно-программное оборудование (маршрутизатор cisco) для организации обмена информацией Агентства с Национальным банком;
   - Периферийное офисное оборудование: принтеры, сканеры.

II. Программное обеспечение

1. На сервере приложений установлена Программное обеспечение «Информационно-аналитическая система по процессу выплаты компенсаций по вкладам».
2. На персональных компьютерах сотрудников Агентства ПК установлены операционные системы Windows 7,10, офисные приложения (Word, Excel и т. д.).
3. Бухгалтерский учёт и отчётность финансово-хозяйственной деятельности Агентства осуществляются средствами программного продукта 1С_8.3. Информационная база данных хранится на сервере Агентства, доступ к базе данных осуществляется только регламентированным сотрудником по ключу доступа. Предусмотрено сопровождение программного продукта 1С_8.3, которое осуществляется разработчиком.
4. Для работы на рынке НБКР с ценными бумагами в онлайн режиме по каналам связи используется аппаратно-программный маршрутизатор (cisco).

III. Информационное взаимодействие и обмен данными

1. Обмен данными и доступ к данным на сервере осуществляется по проводной локальной сети. Доступ к Интернет, эл. почте сотрудников Агентства – по проводной и беспроводной (Wi-Fi) локальной сети.
2. Доступ к базе данных программного комплекса 1С_8.3 разрешен только регламентированным пользователям.
3. Взаимодействие Агентства с НБКР производится по выделенному каналу связи.

IV. Безопасность и защита информации

1. Защита от вирусных заражений обеспечивается антивирусной программой, обновление антивирусной базы осуществляется в автоматическом режиме через каждые 2 дня.
2. В целях предотвращения несанкционированного доступа к пользовательским данным каждому пользователю присвоено уникальное имя (Login) и пароль, на сервере защита данных осуществляется средствами и политиками безопасности сервера.
3. Защита данных и персональных компьютеров при несанкционированных отключениях электричества приобретено для каждого персонального компьютера источники бесперебойного питания.

Программное обеспечение «Информационно-аналитическая система по процессу выплаты компенсаций по вкладам» (ИАС или Система), для автоматизации бизнес-процессов АЗД по:

- сбору отчетности от коммерческих банков и расчету обязательных взносов, штрафов и пени;
- выплате гарантированных сумм вкладчикам банков-банкротов (при наступлении гарантийного случая);
- формированию архива электронных документов по принятым решениям АЗД, в том числе для хранения истории работы с банком агентом.

ИАС не охватывает административно-хозяйствующие операции, такие как расчет заработной платы, кадровый учет, бюджетирование, учет размещения денежных средств ФЗД в ГЦБ и др.

Для бухгалтерского учёта и отчётности внутрихозяйственной деятельности Агентства эксплуатируется имеющийся программный продукт на платформе 1С.

Требование к ИТ-аудиту

Проведение независимого ИТ-аудита и компьютерно-технической экспертизы, включая (но не ограничиваясь):

- архитектуру общесистемного проекта Системы,
- условия эксплуатации Системы,
- используемые базы данных, объекты автоматизации и управления,
- обеспечение информационной безопасности в Системе для получения доказательств и электронных свидетельств о соответствии Системы следующим требованиям:
    - применяемой мировой практики, международных рекомендаций и стандартов в области промышленной разработки программного обеспечения и информационной безопасности,
    - а также специальным требованиям Заказчика, сформулированным в процессе разработки Системы с целью выработки независимого объективного заключения и определения уровня соответствия ИАС:
- требованиям эффективности долгосрочной эксплуатации, в том числе:
    - стоимости эксплуатации, зависящей от выбранных программно-аппаратных решений и требуемой квалификации обслуживающего персонала;

- обеспечение эффективного вертикального и горизонтального масштабирования;
- способность эффективной интеграции с внешними системами;
- обеспечение надлежащей надёжности и отказоустойчивости,

- требованиям по обеспечению информационной безопасности;
- требованиям по отсутствию принципиальных ограничений, связанных с доступностью всех функций, количеством одновременно работающих пользователей, срокам хранения или доступностью обрабатываемой информации;
- требованиям по патентной, интеллектуальной и лицензионной чистоте для любых использованных при создании компонентов Системы.

Основными задачами ИАС является

- Формирование единого хранилища данных в разрезе КБ по предоставленным отчетам, взносам, начисленным штрафам и пени, вкладчикам и выплаченным компенсационным суммам.
- Внедрение механизмов автоматизированной загрузки обязательной ежеквартальной и полугодовой отчетности КБ, реестров вкладчиков в случае наступления гарантийного случая.
- Описание форматов, полей и проверок для входящих отчетов.
- Формирование истории работы с каждым КБ: дата и документы включения в ФЗД, предоставленные отчеты, переписка КБ с АЗД, жалобы и обращения граждан по КБ и др.
- Формирование истории выплат компенсационных сумм по вкладам в разрезе КБ с момента наступления гарантийного случая (уведомления НБКР об отзыве банковской лицензии).
- Формирование истории выбора и работы с Банком-агентом.
- Формирование механизмов выгрузки данных из ИАС в требуемых форматах.
- Определение перечня регламентных выходных отчетов для нужд АЗД.
- Разработка всей документации на поставляемую систему и программы обучения пользователей.

Ожидаемые результаты работ от внедрения ИАС:

- Создание единого центра информации.
- Миграция исторических данных в новую ИАС.
- Внедрение новых технологий сбора, загрузки, очистки и хранения информации.
- Внедрение новых форматов передачи информации от КБ в АЗД.
- Уменьшение времени для поиска, свода и обработки информации.
- Увеличение времени для анализа собранной информации.
- Развитие информационных систем АЗД, обеспечение ее совместимости и взаимодействия с другими государственными информационными системами.

Краткое обозначение указанных работ в настоящем ТЗ.

В тексте настоящего документа используются следующие краткие обозначения оказываемых услуг: «работы», «аудит» и/или «проведение аудита».

- АИС, ИС — информационно аналитическая система, информационная система.
- БД — база данных.
- ИБ — информационная безопасность.

- ОС — операционная система.
- ПО — программное обеспечение.
- Реверс-инжиниринг (от англ. reverse engineering, «обратная разработка») — исследование скомпилированной программы с целью воссоздания принципов и алгоритмов её работы.
- ТЗ — техническое задание.

Плановые сроки начала и окончания работ

Исполнитель должен направить Заказчику проектный вариант «Отчёта о результатах ИТ аудита Системы» (далее — «Отчёт») в течение 21 дня после подписания Договора.

Общий срок доработки «Отчёта» для выпуска в стадию «Финальная версия» при наличии обоснованных возражений Заказчика, исключая периоды проведения дополнительных компьютерно-технических экспертиз, не должен превышать 30 дней после подписания Договора.

Исполнитель должен приступить к работам на собственной территории при наличии исходных данных описанных в данном ТЗ, предоставленных Заказчиком, в течение пяти рабочих дней после даты согласования ТЗ и подписания Договора.

Исполнитель может приступить к работам на территории Заказчика по ссогласованию, но не более пяти дней после подписания Договора.

Порядок предъявления Заказчику результатов работ

Результаты работ сдаются в сроки, установленные Договором и настоящим Техническим заданием.

Исполнитель не позднее срока окончания работы направляет в адрес Заказчика извещение о готовности к сдаче работ по предмету Договора и предоставляет Заказчику проект «Отчёта о результатах ИТ аудита».

Результаты работ отражаются в «Отчёте о результатах ИТ аудита», подписанным представителями Исполнителя и согласованным с представителями Заказчика.

Результаты выполненных работ принимаются Заказчиком с подписанием Акта сдачи-приемки работ.

Результаты проведения работ должны определить качество разработки Системы в соответствии с признанными мировыми практиками, определить степень соответствия Системы определённых в Техническом задании специальным и общим требованиям, определить потенциал эффективности дальнейшей долгосрочной эксплуатации и, в случае применимости, выявить и обосновать наличие системных, архитектурных, эргономических, логических, эксплуатационных и иных несоответствий; обеспечение информационной безопасности при разработке и при работе Системы.

Результаты работ должны привести к независимой оценке соответствия Системы установленным требованиям Технического Задания, по которой производилась разработка АИС, в том числе обеспечению информационной безопасности при разработке и работе Системы; оценке потенциала эффективности дальнейшей эксплуатации; выявлению системных, архитектурных, эргономических, логических эксплуатационных и иных несоответствий и уязвимостей.

Для решения указанных выше задач должны быть проведены следующие работы:

- сбор электронных свидетельств и исходных данных: компьютерные материалы, натурное изучение условий эксплуатации,
- анкетирование и интервьюирование персонала Пользователя Системы с заполнением соответствующих Протоколов, представителей Разработчика;

- сбор любых иных сведений, касающихся аудируемой Системы, необходимых Исполнителю для проведения работ,
- анализ собранных электронных свидетельств, исходных данных и предоставленных документов,
- анализ результатов анкетного опроса и Протоколов интервьюирования,
- анализ системы на отсутствие незадокументированных возможностей,
- оценка проанализированных материалов на предмет соответствия установленным требованиям настоящего Технического задания,
- оценка проанализированных собранных данных и материалов на предмет обеспечения информационной безопасности при разработке и работе Системы,
- оценке потенциала эффективности дальнейшей эксплуатации по её стоимости, обеспечению масштабируемости, способностью к интеграции с внешними системами, обеспечению надлежащей надёжности и отказоустойчивости для систем подобного уровня и масштаба,
- оценке выявленных системных, архитектурных, эргономических, логических, эксплуатационных и иных несоответствий и уязвимостей.

Цели аудита

Система соответствует требованиям Технического Задания, не содержит не задокументированных возможностей и в Системе отсутствуют патентные, интеллектуальные и лицензируемые проблемы. Предполагается, что система обладает соответствующей надёжностью и стабильностью, предполагаемых для систем подобного уровня, обладает способностью к интеграции с внешними системами, отвечает технико-экономическому обоснованию.

Результаты, выраженные в виде отчёта по выполнению выше обозначенных требований по аудиту должны явно говорить о соответствии или несоответствии системы требованиям.

Выполнение работ

Организация-исполнитель должна провести следующие работы в рамках проводимого аудита:

1. Выполнить комплексный ИТ аудит, квалифицированную оценку и компьютерно-технический анализ предоставленных Заказчиком документов, исходных материалов и электронных свидетельств:
    a. техническое задание на разработку Системы и все приложения (переписка, акты, отчёты разработчика) к нему,
    b. системный проект Системы, дизайн (архитектура) баз данных,
    c. специальные требования Заказчика
2. Провести идентификацию всех компьютерно-технических и иных объектов, имеющих отношение к разработке, функционированию или эксплуатации Системы.
3. Провести анкетирование и интервьюирование персонала Пользователя Системы, представителей Разработчика Системы.
4. Провести анализ и оценку Системы, идентифицированных объектов Системы, условий эксплуатации в соответствие с требованиями Технического задания.

5. Подвергнуть компьютерно-технической экспертизе (включая этап реверс-инжиниринга) и квалифицированной оценке собранные, выявленные в результате анализа или в ходе проведения работ материалы на предмет соответствия требованиям Технического задания.
6. Подвергнуть экспертизе и квалифицированной оценке надёжность и отказоустойчивость Системы
7. Провести прогнозную оценку рисков, связанных с реализованными в Системе требованиями информационной безопасности.
8. Выполнить сбор и квалифицированную оценку иных сведений, необходимых Исполнителю для достижения цели выполнения работ.
9. Обследование состояния сервера, анализ функционирования серверного оборудования и соответствия требованиям, анализ состояния активного и пассивного сетевого оборудования, кабельной системы, анализ источников бесперебойного питания, их достаточности, Проверка осуществления резервного копирования, доступа к интернету, почтового сервера, антивирусной защиты, защита от несанкционированного доступа, обследование установленного программного обеспечения на компьютерах и на сервере, обследование каналов передачи данных с банками-участниками и другими контр агентами Агентства, анализ работы телефонии, анализ работы и настроек корпоративной электронной почты, обследование использующихся систем информационной безопасности, проверка работы антивирусной защиты и антиспам защиты электронной почты.

Аудит систем безопасности:

- обследование использующихся систем информационной безопасности;
- проверка работы антивирусной защиты и антиспам защиты электронной почты;
- обследование систем защиты от взлома инфраструктуры;
- анализ возможных путей доступа к информации компании;
- обследование межсетевых настроек безопасности;
- анализ настроек сетевых политик;
- анализ системы хранения и бэкапирования данных.

Общие технические требования.

При проведении работ по аудиту ИТ-инфраструктуры предприятия требуется обеспечить на время проведения всех инструментальных обследований оборудования и информационных систем их безотказную и бесперебойную работу в момент проведения исследований.

При проведении исследований должны использоваться только лицензированные и сертифицированные необходимым образом аппаратные и программные продукты.

Все съемные носители Исполнителя, используемые при проведении аудита должны быть свободны от вирусов и прочих вредоносных программ.

Требования к проведению выполняемых работ.

При проведении аудита должны использоваться как опросные (опросные листы, анкеты, интервью), так и инструментальные средства (программные и аппаратные тестеры оборудования и программного обеспечения).

Результаты работ

Исполнитель должен разработать и предоставить для согласования проект Отчёта и Отчёт в соответствие с требованиями по порядку предъявления результатов работ, описанными в ТЗ.

Результаты работ должны быть изложены в «Отчёте о результатах ИТ-аудита», подписанным представителями Исполнителя.

«Отчёт о результатах ИТ-аудита» должен быть выпущен в одну стадию «Финальная версия» и содержать (но не ограничиваться) следующие взаимоувязанные блоки:

1. Резюмирующее описание выявленных результатов ИТ-аудита.
2. Результаты анализов и компьютерно-технических экспертиз.
3. Анкеты и Протоколы интервьюирования, а также анализ по ним
4. Обоснованные выводы, обобщающие результаты анализа и содержащие квалифицированную оценку уровня соответствия Системы и неразрывно связанных с нею компонентов:

4.1. применимым требованиям Технического задания,

4.2. требованиям эффективности долгосрочной эксплуатации, в том числе:

4.2.1. стоимости эксплуатации, зависящей от выбранных программно-аппаратных решений и требуемой квалификации обслуживающего персонала,

4.2.2. обеспечение эффективного вертикального и горизонтального масштабирования,

4.2.3.способность эффективной интеграции с внешними системами,

4.2.4.обеспечение надлежащей надёжности и отказоустойчивости,

4.2. требованиям по обеспечению информационной безопасности,

4.3. требованиям по отсутствию принципиальных ограничений, связанных с доступностью всех функций, количеством одновременно работающих пользователей, срокам хранения или доступностью обрабатываемой информации

4.4. требованиям по патентной, интеллектуальной и лицензионной чистоте для любых использованных при создании компонентов Системы.

5. Оценка рисков информационной безопасности Системы,
6. Оценка по наличию не задокументированных возможностей,
7. Исчерпывающий реестр информационных систем, объектов и ресурсов в составе информационного окружения Системы.
8. Оценка соответствий Системы требованиям Техническим Заданием, а также требованиями данного ТЗ.

Результатом предъявления «Отчёта» должно стать письменное подтверждение со стороны Заказчика о соответствии предоставленного «Отчёта» требованиям настоящего Технического задания, выраженное в виде Акта сдачи-приёмки работ.

Квалификационные требования к Исполнителю

Аудиторская организация-исполнитель должна:

1. иметь соответствующую лицензию на территории Кыргызской Республики, а также иметь опыт аудиторской деятельности в области ИТ не менее 3-х лет;
2. быть независимым от Заказчика, Пользователя и Разработчика Системы;

- иметь в штате не менее 2-х ИТ-аудиторов соответствующей квалификации (Копии лицензий и сертификатов);

3. назначить руководителем аудита информационных систем для проведения аудита информационных систем, обладающего квалификационным сертификатом в области ИТ аудита;
4. в связи с потенциальным доступом к конфиденциальным сведениям, составляющим охраняемую Законом КР тайну, обеспечить проведение работ, связанных с доступом к объектам аудита, содержащих такие сведения, исключительно сотрудниками, являющимися гражданами Кыргызской Республики.
5. Резюме компании с указанием опыта реализации подобных проектов;
6. Описание планируемой работы (не более 10 страниц);
7. Календарный план реализации проекта;
8. Ресурсный план реализации проекта (с указанием чел. часов);
9. Коммерческое предложение, включающее в себя:
   – Стоимость проекта;
   – Условия оплаты;
   – Дату готовности к началу работ.

Ограничение ответственности Исполнителя

Ответственность Исполнителя ограничивается изучением, анализом электронных свидетельств, всевозможных материалов, данных и информации, собранных самостоятельно или предоставленных Заказчиком в рамках, ограниченных настоящим Техническим заданием.

Исполнитель не ограничивается в выборе программно-технических средств для проведения анализа и дачи заключений по собранным или предоставленным электронным свидетельствам и материалам. Исключение составляет соблюдении законодательства Кыргызской Республики при сборе электронных свидетельств, всевозможных материалов, данных и информации

В случаях отсутствия надлежаще собранных материалов, данных и информации, утраты или порчи существенных свидетельств (документов, иных материалов), делающих невозможным выработку заключения по Системе и соответствия требованиям Заказчика к результатам работ (п. 4.1, 4.2), Исполнитель обязан отразить в «Отчёте» объективные причины, препятствующие выполнению работ согласно требованиям Технического Задания. Исполнитель обязуется предоставить в целости и сохранности первоначальные образы, по которым проводилась вся работа по данному Техническому Заданию для возможности перепроверки информации, отражённой в Отчёте по аудиту

Ограничение ответственности Заказчика

Заказчик готовит и предоставляет Исполнителю доступные для передачи в электронном виде исходные данные, электронные свидетельства и другие материалы, требующиеся исключительно для целей проведения работ:

1. Описание, паспорта, схемы и топологии информационных активов и информационного окружения Системы:
   1.1. ресурсы,
   1.2. сотрудники,

1.3. инфраструктура,
1.4. оборудование,
1.5. программное обеспечение,
1.6. инструменты, используемые в работе Системы.

2. Документация по Системе:
   2.1. Техническое задание на разработку и приложения к нему,
   2.2. Документация разработчика,
   2.3. Инструкции администратора, пользователя Системы,
   2.4. Инструкции по эксплуатации и сопровождению Системы.

Прочие условия

Настоящее Техническое задание может быть уточнено в процессе проведения работ исходя из изменившихся требований Заказчика, которые могли быть не сформулированы на этапе разработки Технического задания.

Если в ходе проведения работ будет выявлено, что состояние информационного окружения и информационных активов Системы не подлежат компьютерно-технической экспертизе по причине технического несовершенства, утраты существенных электронных свидетельств, исходных данных и материалов, противодействия со стороны исполнителей Пользователя, Разработчика или Заказчика, существенных искажений в документации, файлах, журналах действий и настройках, отсутствия надлежащим образом подготовленной документации или материалов, и/или по иным причинам, не позволяющим провести аудит должным образом, отклонения от настоящего ТЗ должны быть согласованы с Заказчиком и Исполнителем в установленном порядке.

Исполнитель, при невозможности выполнения данного ТЗ при отсутствии квалификации, собственных технических возможностей, отсутствию соответствующих специалистов, либо при наступлении других причин, сообщить официальным письмом на имя Заказчика о невозможности исполнения условий договора. Заказчик оставляет за собой право взыскания с Исполнителя неустоек и запуска собственных процедур по подобным ситуациям.

Настоящее техническое задание является проектом и не утверждена. В процессе согласования и утверждения могут быть внесены изменения.