

ОТЧЕТ о результатах пилотного аудита информационной системы “IS Казна.Бюджет”

1. Резюме

Отсутствие видения является одной из серьезных проблем, обнаруженных в ходе проверки. Стратегия развития информационных технологий (далее ИТ стратегия) крайне необходима, чтобы уменьшить риски, связанные с информационной безопасностью, нехваткой ресурсов, управления активами.

В результате выполненных процедур мы обнаружили ряд нарушений, которые привели нас к следующим выводам:

- отсутствие координации действий между Министерством финансов КР (МФКР), Центральным Казначейством (ЦК МФКР) и Государственным учреждением “Инфосистема” (ГУИС) относительно функционирования информационной системы “IS Казна.Бюджет”. Нет единой системы утверждения положений, регламентов и политик (стр. 15. Наблюдение 1).
- Отсутствие контроля со стороны МФ КР над процедурой найма и увольнения сотрудников ГУИС. Штатное расписание утверждается только директором ГУИС без согласования с МФКР (стр. 19. Наблюдение 7).
- Отсутствие мониторинга и контроля работы системы Service Desk Naumen относительно процедуры закрытия запросов (стр. 22. Наблюдение 10).
- Отсутствие утвержденного Технического задания на разработку “IS.Казна.Бюджет” с указанием требований к работе системы со стороны МФКР и ЦК (стр. 24. Наблюдение 13).
- Обнаружены значительные риски в области информационной безопасности, связанные с несанкционированным доступом к информации, оборудованию и в Центр обработки данных, риски возможной утечки информации, заражения вирусом (стр. 29. Наблюдение 25).
- Слабый контроль управления основными средствами (стр. 30. Наблюдение 27).
- Обнаружены факты внесения изменений в отчеты 2014 года после окончания отчетного периода (стр. 34. Наблюдение 33).

В заключение, мы бы хотели отметить, что вышеперечисленные выводы предоставлены не для того, чтобы Министерство финансов КР принимало меры по решению каждой из проблем отдельно, а для того, чтобы подчеркнуть, что Министерство финансов КР недостаточно подготовлены к тому, чтобы принять решение о покупке новой информационной системы для Казначейства или о совершенствовании действующей системы " IS Казна.Бюджет 1.0" в целях реализации плана действий, указанного в статье 62 Постановления Правительства №26 от 26.01.2011.

2. Введение

2.1 Глобальная программа обучения Инициатива развития ИНТОСАИ

Согласно Соглашения о сотрудничестве, подписанного между Счетной палатой КР и инициативой развития ИНТОСАИ (INTOSAI Development Initiative), Счетная палата КР дала согласие на участие в “Глобальной программе обучения IDI по проведению специализированных аудитов - аудита информационных технологий /систем.”

Данная программа включает две фазы: теоретический курс дистанционного обучения и курс практического обучения путем проведения пилотного аудита ИТ. Данная

программа подготовлена с учетом передового опыта и руководства по аудиту ИТ, включенных в “Справочник рабочей группы IDI по аудиту ИТ”.

2.2. Выбор темы аудита и подготовка отчета предварительного изучения

Для прохождения обучения и проведения пилотного аудита была создана аудиторская группа, которая провела следующие аналитические мероприятия по отбору объекта для проведения пилотного аудита ИТ:

1. Были составлен предварительный список из трех организаций, где установлены и функционируют информационные системы: Государственная регистрационная служба при Правительстве КР, Министерство финансов КР (Центральное казначейство) и Социальный фонд КР.
2. Был подготовлен Опросный лист и направлен в отобранные организации.
3. Были получены заполненные Опросные листы с приложенными документами.
4. Установлены следующие критерии отбора:
 - результаты таблицы ранжирования;
 - информация, полученная из предыдущих отчетов;
 - социально-экономическая значимость;
 - запросы государственных учреждений.

В результате предварительного изучения был отобран объект для проведения ИТ аудита– Информационная система “IS Казна. Бюджет -1.0”, разработанная специалистами Государственного учреждения “Инфо-система” при Министерстве финансов КР.

Отчет предварительного изучения, а также План аудита, утвержденный Советом Счетной палаты КР 9 сентября 2014 года был предоставлен в Интосаи.

2.3 Мандат аудита

- Мандат ВОФК для проведения ИТ аудита содержится в Международных стандартах ВОФК I- Лимская декларация (Часть VII, Статья 22).
*“Статья 22. Проверка оборудования по электронной обработке данных
Уровень расходов на оборудование по электронной обработке данных требует также надлежащей проверки. Такие проверки должны носить системный характер, при этом особое внимание должно быть уделено планированию потребности, экономному использованию электронного оборудования, использованию контингента специалистов необходимой квалификации, подобранных предпочтительно из состава администрации проверяемой организации, предотвращению неправильного использования техники, полезность получаемой информации.”*
- СП КР проводит аудит с учетом положений статьи 107 Конституции Кыргызской Республики и статей 4 и 5 “Закона о Счетной палате Кыргызской Республики”.
- Счетная палата Кыргызской Республики осуществила пилотный аудит информационной системы “IS казна. Бюджет -1.0” с 3 ноября 2014 по 15 апреля 2015 года на основании приказа № 04- 6/404 от 31 октября 2014 года.

2.4 Стандарты аудита

Счетная палата Кыргызской Республики осуществляет аудит в соответствии с Национальными стандартами государственного аудита, утвержденными Постановлением Совета Счетной палаты Кыргызской Республики от 31 марта 2008 года № 01-9/ 14.

СП КР не проводила аудит хозяйственной деятельности Министерства финансов КР, Центрального Казначейства при Министерстве финансов КР и Государственного учреждения “Инфо-Система» при Министерстве финансов КР.

2.5 Ответственность руководства

За полноту, достоверность и объективность, представленных и использованных в ходе аудита сведений, информации, материалов и документов, согласно статье 29 Закона Кыргызской Республики «О Счетной палате Кыргызской Республики», персональную ответственность несут руководство и соответствующие должностные лица Министерства финансов КР и Государственного учреждения «Инфо-Система» при Министерстве финансов КР.

2.6 Перечень ответственных лиц

Аудит проводился с согласия Статс-секретаря Министерства финансов КР- Баямановой З.Э и Директора ЦК МФКР Бакетаева А.К и в присутствии начальника Управления информационных технологий и модернизации МФКР Дуйшембиевой Н и директора ГУИС Токочева Р и других сотрудников Министерства финансов КР .

2.7 Перечень изученной документации.

Перечень изученных регламентов, положений и инструкций предоставлен в **Приложении 1**.

2.8 Выполненные процедуры.

В рамках ИТ аудита были выполнены следующие процедуры:

- Интервью с сотрудниками МФКР, ЦК МФКР, ГУИС, РОК;
- Анализ организационной структуры ЦК и ГУИС;
- Анализ внутренних политик, процедур, положений и инструкций МФКР, ЦК МФКР, ГУИС;
- Анализ нормативных актов, регулирующих деятельность системы казначейства по кассовому исполнению государственного бюджета;
- Анализ организационных мер в области информационной безопасности ЦК МФКР и ГУИС;
- Анализ текущего обеспечения физической безопасности ЦОД, РЦОД;
- Анализ прав доступа сотрудников в ИС;
- Анализ и оценка функциональности ИС на соответствие требованиям нормативных актов МФКР и ЦК МФКР;
- Анализ отчетов “Service Desk Наумен”;
- Тестовое восстановление резервной копии;
- Проверка наличия физических активов в виде инвентаризации;
- Составление списка предварительных результатов (в виде наблюдений);
- Разработка рекомендаций по минимизации обнаруженных рисков.

2.9 График проведения аудита.

Name	Занимаемая должность	Фактические (чел дни)				
		Сбор документов и подготовка предварительного отчета	Полевые работы	Подготовка проекта отчета	Окончательный отчет	Итого
Дуйшенкул кызы Д.	Аналитик.	15	80	60	20	175
Мурзалиев А.	Гл. инспектор.	5	20	5	5	35

Сооданбеков Ч.	Референт	15	60	10	0	85
Котельников К.	Внешний специалист	10	20	30	10	70
Арстанбек уулу К.	ИТ специалист	5	5	0	10	20
Токгасунова Б.	Аналитик	10		0		10
Итого		60	185	105	45	395

3. Цели, задачи и критерии аудита

Главная цель данного аудита – получение гарантий того, что Министерство финансов КР, в том числе Центральное Казначейство при МФ КР, имеют адекватные и эффективные процессы управления информационной системой, отвечающей целям и задачам организации.

Согласно утвержденной программе основными задачами аудита являются:

Область аудита		Задачи и критерии аудита.
ИТ Управление	Организационная структура, политики и процедуры	Провести оценку того, насколько организационная структура, утвержденные положения и регламенты отвечают целям организации при использовании ИС.
	Внутренний контроль	Провести оценку для получения подтверждения о действующей системе внутреннего контроля в организации.
	Человеческие ресурсы & Ресурсы	Определить насколько соответствующим образом квалифицированный и обученный персонал нанят на работу и что они имеют соответствующий доступ к ресурсам, которые позволяют организации достигать свои цели.
ИТ Операции	Управление услугами	Провести оценку того, насколько активно организация проводит мониторинг ИТ операций, указанных в Соглашении и документах, регламентирующих работу ИС.
	Управление изменениями	Использует ли организация утвержденные процедуры для осуществления контроля за всеми изменениями, вносимыми в ИС и его приложения.
Разработка & Закупка	Требования организации	Убедиться в том, что отчеты разработчиков системы соответствуют требованиям пользователей системы, утвержденных в виде Инструкций.
Информационная безопасность	Политика безопасности	Провести анализ того, описаны ли в политике безопасности ИТ требования, которым должны следовать организация и ее сотрудники для защиты технических и информационных ресурсов
	Организация безопасности ИС	Подтвердить безопасность операционной деятельности процесса обработки ИС.
	Коммуникации & Управление операциями	Получить подтверждение безопасности организации внутренних и внешних коммуникаций.

	Управление активами	Имеет ли организация соответствующую систему управления активами, которая обеспечивает ее информационную безопасность?
	Физическая безопасность	Обеспечивает ли система управления активами защиту от краж или повреждений ИТ-оборудования, несанкционированного доступа, копирования или просмотра конфиденциальной информации?.
	Контроль доступа	Убедиться в том, что только авторизованные пользователи имеют доступ к соответствующей информации.
Контроль приложений	Контроль ввода	Оценить, насколько достоверные данные в настоящее время вводятся в приложения ИС уполномоченным лицом.
	Обработка	Оцените, обеспечивает ли ИС целостность, достоверность и надежность данных на протяжении всего цикла обработки данных.
	Выходные данные	Оцените, обеспечивает ли ИС полноту и достоверность выходной информации перед ее дальнейшим использованием и необходимую защиту.
	Безопасность данных ИС	Оцените, правильно ли защищена информация от нецелевого использования.

4. Охват аудита и методология

4.1 Основные объекты аудита

4.1.1 Министерство финансов Кыргызской Республики (МФКР);

Заказчиком и правообладателем информационной системы "IS:Казна.Бюджет" (далее ИС) является Министерство финансов КР в лице Центрального Казначейства при МФ КР.

Согласно Приказа МФ КР от 18 декабря 2013 года №206-П, функционирование ИС было регламентировано следующими документами:

- Регламент сопровождения ИС «IS:Казна. Бюджет»;
- Регламент подключения, управления доступом и технической поддержки пользователей информационной системы - "IS:Казна.Бюджет".

Управления информационных технологий и модернизации МФКР.

В целях осуществления технической поддержки и сопровождение информационных систем МФКР, а также координация вопросов по реализации и внедрению Информационных систем управления государственными финансами (ИСУГФ), было создано Управление информационных технологий и модернизации МФКР (далее – Управление), действующее на основе Положения, утвержденного Приказом МФКР.

Основными функциями Управления являются:

- обеспечение непрерывной деятельности информационных систем Министерства;
- координация процесса внедрения информационных систем управления государственными финансами и обеспечение безопасности информации в Министерстве.

Управление возглавляет руководитель управления и состоит из отдела и сектора:

1. Отдел технической поддержки (4 шт.ед.):

- заведующий отделом – 1 шт.ед.;
- главный специалист – 1 шт.ед.;
- ведущий специалист – 1 шт.ед.;
- специалист – 1 шт.ед.

2. Сектор модернизации (3 шт.ед.):

- заведующий сектором – 1 шт.ед.;
- главный специалист – 1 шт.ед.;
- ведущий специалист – 1 шт.ед.

Во исполнение пункта 3 приказа Министерства от 22 июля 2013 года №125-П «О мерах по устранению и предотвращению возможных хищений и обеспечения прозрачности исполнения государственного бюджета» и согласно Акт приема-передачи ГУИС передал Управлению ПО "Конфигурация 1С - Администрирование" и функцию администрирования пользователей по предоставлению доступа к ПО "18:Казна.Бюджет".

4.1.2 ЦК МФКР.

Центральное Казначейство Министерства финансов Кыргызской Республики (ЦК МФКР) и его региональные отделения является основным пользователем ИС.

4.1.3 Государственное учреждение “Инфо-система” при МФКР.

Разработку и техническую поддержку ИС осуществляет ГУИС при МФ КР, который разработал собственные положения и инструкции по техническому сопровождению ИС, информационной безопасности, которые не были одобрены МФКР - собственником ИС.

Основными документами, регламентирующими деятельность ГУИС, являются:

1. Указ Президента Кыргызской Республики "О вопросах Центрального казначейства Министерства финансов Кыргызской Республики" от 20 ноября 2008 года N 410.
2. Указ Президента Кыргызской Республики от 11 июля 2012 года УП№136 "О внесении изменений в Указ 1. Указ Президента Кыргызской Республики "О вопросах Центрального казначейства Министерства финансов Кыргызской Республики" от 20 ноября 2008 года".
3. Положение о государственном учреждении "Инфо-Система" при Министерстве финансов Кыргызской Республики, утвержденное Постановлением Правительства Кыргызской Республики от 20 февраля 2012 года № 114 (далее Положение).
4. Соглашение о безвозмездном оказании услуг от 30 декабря 2011 года, подписанное между ЦК МФКР (директор Темирбеков М.) и ГУИС (директор Шаикова А.) (далее Соглашение).
5. Свидетельство о государственной регистрации юридического лица серии ГР № 0063711 от 3 июня 2009 года, выданного Управлением юстиции г. Бишкек Министерства юстиции Кыргызской Республики.

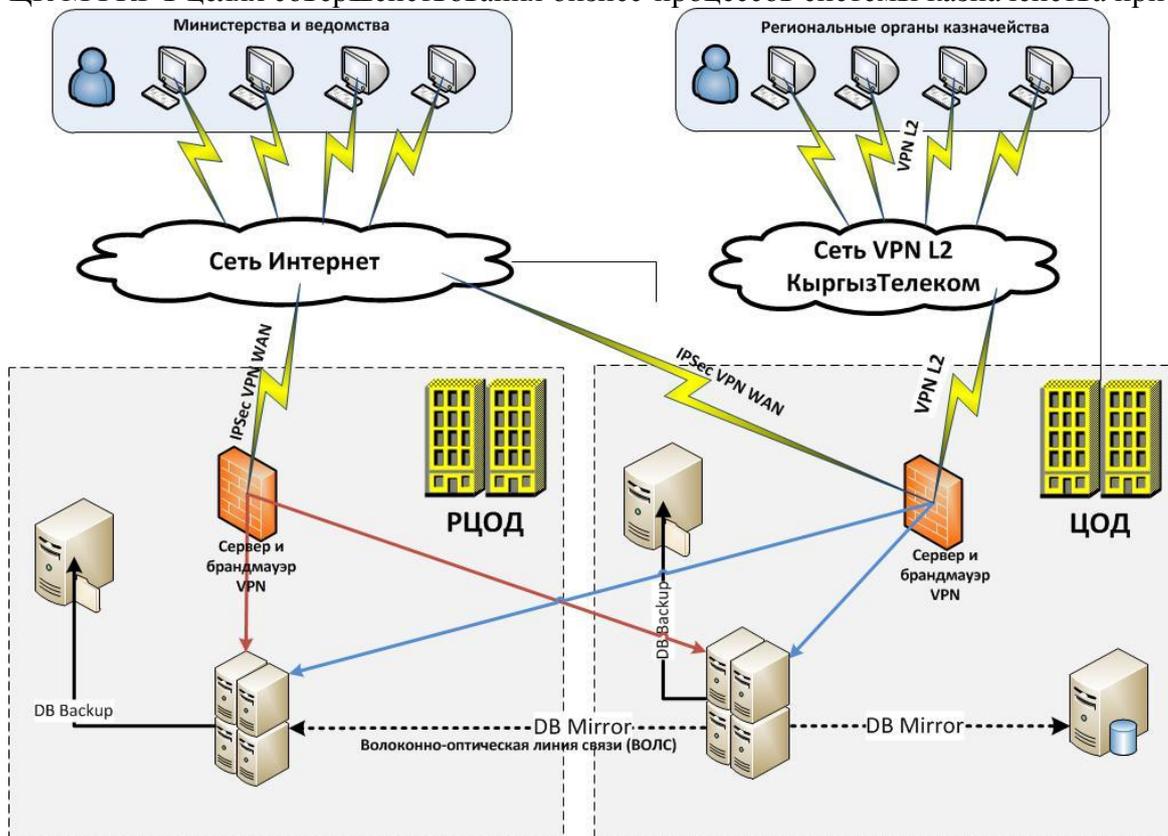
4.2 Описание информационной системы “IS:Казна.Бюджет”

Информационная система «IS:Казна.Бюджет-1.0» (далее ИС) реализована на платформе «1С:Предприятие 8.1» и «Java EE». В ИС входная форма данных по

расходным операциям доступен через приложение на базе платформы «1С:Предприятие 8.1», выходная форма отчетности по заданным критериям реализована на платформе «Jasper Reports».

ИС используется при выполнении государственных функций и предназначена для поддержки рабочих процессов системы казначейства, а также обеспечивает информационное взаимодействие органов казначейства с бюджетными учреждениями КР.

Внедрение данной системы было начато с начала 2011 года по поручению Директора ЦК МФКР в целях совершенствования бизнес-процессов системы казначейства при



создании Единого казначейского счёта, переход который был предусмотрен в Плане мероприятий «Экономика и безопасность», утверждённом постановлением ПКР от 26.01.2011г. №26.

5. Заключение аудита и рекомендации

5.1 Управление ИС

5.1.1 Организационная структура, политики и процедуры

Основной целью данного вопроса является получение доказательств того, что разработанные положения и регламенты отвечают требованиям функционирования ИС.

Наблюдение 1.

Отсутствие координации действий между МФ КР, ЦК МФКР и ГУИС по вопросу функционирования ИС. Отсутствует единая система утверждений положений, регламентов и политик. Нам были предоставлены документы, регламентирующие деятельность ИС, подписанные разными руководителями от имени МФ КР, ЦК МФКР и ГУИС (список НПА в Приложение 2 прилагается). Политики и процедуры,

разработанные ГУИС, не были утверждены МФ КР. Некоторые регламенты и положения не были обновлены с 2011 года.

Риск.

Принятие несогласованных решений ведет к серьезным проблем при работе ИС.

Лучшие практики.

Согласно лучшим мировым практикам, рекомендуется создать Наблюдательный или Технический совет по информационным технологиям при непосредственном руководстве Министра финансов КР или уполномоченного заместителя и в составе ключевых сотрудников. Совет должен обладать функциями определения основной стратегии развития ИТ, разработки и утверждения регламентов и положений, решения вопросов о закупках новых ИС или совершенствовании действующей ИС.

Рекомендация.

МФ КР должен создать механизм, который предоставит ему возможность осуществлять контроль и мониторинг решения ключевых вопросов, касающихся стратегии развития информационных технологий, установления приоритетов основных требований к системе, системы безопасности ИС, утверждения регламентов и положений, мониторинга условий предоставления информационных услуг и улучшения качества предоставления информационных услуг. МФ КР должен также провести ревизию всех регламентов и положений, относящихся в деятельности и технического обслуживание ИС “IS Казна.Бюджет”.

Наблюдение 2.

Согласно условиям главы 5 (пункт 19) Положения о государственном учреждении "Инфо-Система" при Министерстве финансов Кыргызской Республики утвержденного Указом Правительства КР #114 от 20 февраля 2012 года *“учреждение осуществляет свою деятельность на основе самостоятельно разработанных планов работы. Перспективные, годовые и текущие планы работы учреждения утверждаются Министерством по согласованию с Центральным казначейством МФ КР”*.

Согласно условиям главы 2 (пункта 7) основной задачей деятельности ГУИС является предоставление информационно-коммуникационных услуг не только системе казначейства и государственным органам по организации учета и управления персоналом государственной службы, а также внедрение и поддержка автоматизированных информационных систем в государственных органах Кыргызской Республики.

В **Приложение 2** показана таблица с перечнем всех программных продуктов, разработанных специалистами ГУИС за период с 2009 по 2012.

Аудитом отмечено, что условия пункта 19 Положения **не выполняются**, так как перспективные, годовые и текущие планы работы ГУИС, включающие разработки не только для МФКР, но и для других государственных учреждений не утверждаются МФКР.

Риск.

МФКР и другие государственные учреждения не имеют плановых показателей для осуществления оценки деятельности работы ГУИС.

Рекомендация.

ГУИС должен осуществлять свою деятельность на основе плана работ, утвержденного МФ КР и ориентированного на выполнение конкретной задачи. Потребность в разработчиках системы должна напрямую зависеть от поставленной задачи и плана работы.

Наблюдение 3.

Согласно условиям Соглашения о безвозмездном оказании услуг между МФКР и ГУИС, ГУИС **ежеквартально** передает результаты выполненных работ по акту приема-передачи

с приложением сопроводительных/пояснительных документов. Одновременно передаются ключи (коды доступа) и технические документации (пункт 1.3). Акт приемки работ предоставляется Исполнителем (ГУИС) не позднее 3 (трех) рабочих дней после завершения выполнения услуг (пункт 5.2).

Данные условия Соглашения не выполняются.

Риск.

Отсутствие квартальных отчетов и Актов выполненных услуг, не дает возможности МФ КР осуществлять контроль и мониторинг качества услуг, предоставляемых ГУИС согласно условиям Соглашения.

Рекомендация.

МФ КР и ЦК МФКР должны принять меры по выполнению условий Соглашения, а получению квартальных отчетов и подписании Актов выполненных услуг с передачей кодов.

Наблюдение 4.

Согласно пункту 27 Положения источниками финансирования ГУИС являются отчисления в размере 0,1 процент от годовой уточненной суммы сметы расходов по бюджетным средствам на отчетный финансовый год **за исключением:**

- Аппарата Президента Кыргызской Республики, Аппарата Правительства Кыргызской Республики, Управления делами Президента Кыргызской Республики и его подведомственных организаций, Аппарата Жогорку Кенеша Кыргызской Республики, Управления делами Жогорку Кенеша Кыргызской Республики;
- бюджетных учреждений, финансируемых из местного бюджета;
- статей расходов бюджетных учреждений, таких как заработная плата, отчисления страховых взносов по государственному социальному страхованию, социальные пособия, стипендии и категориальные гранты.

Общая сумма финансирования за период с 2009 по 2014 годы составила 146279,2 тыс. сомов.

Финансирование и расходы ГУИС на период с 2009 по 2014 год (тыс. сом)					
№	год	Остаток на начало	приход (0.1%)	расход	Остаток на конец
1	2009	0	13,887.1	8,339.6	5,547.5
2	2010	5,547.5	17,100.3	18,484.0	4,163.8
3	2011	4,163.8	24,234.3	22,924.5	5,473.6
4	2012	5,473.6	35,387.1	38,850.9	2,009.8
5	2013	2 009,8	28 184,5	29 872,9	318,0
6	2014	318,0	27 485,9	26 282,3	1 521,6
	Итого		146 279,2	144 754,2	1 521,6

Как со стороны МФКР, так и со стороны других государственных учреждений отсутствует контроль расходования средств ГУИС.

Финансирование ГУИС осуществляется из средств государственного бюджета не напрямую, а косвенно, то есть через государственные учреждения, которые осуществляют оплату в размере 0.1% от своего бюджета на счет ГУИС (Схема финансирования в

Приложение 3), но при этом активы и обязательства учреждения не включаются в сводный государственный баланс.

Риск.

Риск не достижения задач и целей, поставленных перед МФ КР и ЦК МФКР, а также необоснованного увеличения суммы расходов.

Рекомендация.

МФ КР и ГУИС должны принять срочны меры по изменению условий финансирования ГУИС, а именно, предусмотреть финансирование ГУИС за счет средств республиканского бюджета отдельной строкой. Прямая форма финансирования предоставит возможность МФКР осуществлять оплату разработчикам ИС на основе актов выполненных услуг, при котором МФКР будет иметь возможность осуществлять контроль за тем, чтобы услуги были предоставлены в соответствии с установленными требованиями, своевременно, качественно и с наименьшими затратами.

Наблюдение 5.

В связи с задержкой поступления средств, на конец каждого года, начиная с 2009, имеется задолженность по социальным отчислениям, а сумма штрафных санкций составила 1,554,5 тыс. сом, которые должны быть выплачены из средств бюджета

Задолженность по социальным отчислениям							
	Обязательства плательщика	Суммы обязательств на конец (тыс. сом):					
		2009	2010	2011	2012	2013	2014
1	Страховые взносы (кроме НПФ)	31,9	882,5	2 592,6	2 207,9	3 619,2	3 277,3
2	Накопительный пенсионный фонд	0,0		116,0	62,7	69,1	398,9
3	Пени и штрафы	0,0		424,0	158,4	367,3	604,8
	Итого	31,9	882,5	3 132,5	2 429,0	4 055,6	4 281,0

Риск.

Задержка выплат по социальным отчислениям ведет к увеличению расходов в виде штрафных санкций.

Рекомендация.

МФКР и ГУИС должны предпринять срочные меры по погашению задолженности по социальным отчислениям.

5.1.2 Система внутреннего контроля

Основной целью данного вопроса является получение доказательств того, что все рекомендации, указанные в отчете аудиторской компанией Ernst&Young от 6 июня 2011 года, были исполнены и дать оценку системе внутреннего контроля. Аудит не давал оценку рекомендациям, предоставленным аудиторской компанией Ernst&Young.

Наблюдение 6.

Отсутствует система внутреннего контроля. МФ КР и ЦК МФКР не осуществляли контроль исполнения рекомендаций, предоставленных аудиторской компанией

Ernst&Young от 6 июня 2011. Многие комментарии ГУИС о выполнении рекомендаций не были подтверждены ЦК МФКР и ИТ управлением МФ КР. Согласно комментариям ГУИС, многие отсутствующие отчеты об исполнении бюджетов были разработаны. Подтверждения данного факта в виде актов выполненных услуг, подписанных между ГУИС и МФ КР не были предоставлены. Согласно комментариям ГУИС, были внесены изменения в регламенты и политики, которые не были согласованы с МФ КР и ЦК МФКР.

Риск.

Принятие несогласованных решений ведет к дублированию исполнения рекомендаций и дополнительным затратам ресурсов.

Рекомендация.

МФ КР, ЦК МФКР и ГУИС принять меры по согласованию действий при выполнении рекомендаций, предоставленных предыдущим аудитом. МФКР, ЦК МФКР и ГУИС должны принять меры по утверждению всех изменений, внесенных в политики и регламенты на основе рекомендаций предыдущего аудита.

5.1.3 Персонал и ресурсы.

Основной целью данного вопроса является получение доказательств того, что МФКР и ЦК МФКР, являясь заказчиком и пользователем ИС, обладают достаточными ресурсами для управления и технической поддержки ИС.

Наблюдение 7.

Согласно условиям Соглашения о безвозмездном оказании услуг между МФКР и ГУИС, ГУИС несет ответственность за

- оказание консультационной поддержки ЦК МФКР в рамках функционирования ИС «1S:Казна.Бюджет»;
- выполнение работ по технической поддержке ИС «1S:Казна.Бюджет»;
- выполнение функций администратора ИС «1S:Казна.Бюджет» для технического сопровождения, обеспечения информационной безопасности хранимых данных и выполнения резервного копирования базы данных ИС;
- оказание услуг по разработке / внесению изменений ИС «1S:Казна.Бюджет» на основании формализованных требований ЦК при МФКР;
- оказание услуг по обеспечению бесперебойного функционирования ИТ-инфраструктуры Центра обработки данных и Резервного центра обработки данных МФКР .
- ГУИС обеспечивает правильность и бесперебойность функционирования ИС «18:Казна.Бюджет» (пункт 8.2)

Аудитом было отмечено, что ГУИС нарушил условия Соглашения, приняв в конце 2014 года самостоятельное решение об увольнении региональных сотрудников, ответственных за оказание технической поддержки РОК. С сентября 2014 года только 2 человека вместо 53 несут ответственность за техническое сопровождение работы ИС в РОКах. ГУИС обосновал принятие данного решения задержкой финансирования.

Согласно информации, полученной от ГУИС, с сентября 2014 не было отмечено никаких серьезных проблем, связанных с технической поддержкой ИС в РОКах, что дает повод. Сделать вывод о том, что прием на работу 30 региональных сотрудников для 53 РОК не были правильно обоснованы.

Следует также отметить, что сокращения численности штата ГУИС не повлекло за собой

сокращений финансирования ГУИС, так как, прямая зависимости между финансирование и расходами ГУИС **отсутствует**.

Аудитом было установлено, что МФКР и ЦК МФКР не принимали участие при принятии решений по кадровым вопросам ГУИС, так как штатное расписание ГУИС утверждалось директором ГУИС без согласования с МФКР и ЦК МФКР.

ГУИС не предоставил описание кадровой политики, включающей описание процедур приема на работу или увольнения сотрудников ГУИС, план обучения. Процедура приема на работу сотрудников не связана напрямую с выполнением конкретной задачи.

Ниже дана таблица фактического количества специалистов, принятых на работу ГУИС в период с 2009 по 2014 годы.

		Фактическое количество специалистов, принятых на работу ГУИС *					
		2009	2010	2011	2012	2013	2014
1	АУП	5	5	5	12	11	11
2	МОП			6	6	5	2
3	Отдел информационных систем	4		7	7	7	6
4	Отдел разработки программного обеспечения	9		10	9	9	5
5	Отдел региональной поддержки	3	4	2	1	1	
6	Отдел технического развития и поддержки	6		2			
7	Отдел управления проектами	1	1	1	5	4	4
8	Служба информационной безопасности			0	1	1	
9	Служба технической поддержки	4	4	4	6	13	9
10	По трудовому соглашению	56	76	75	81	72	50
	Итого	88	90	112	128	123	87

* таблица подготовлена на основе данных о выплатах, предоставленных ГУИС.

Риск.

Отсутствие четкой кадровой политики приведет к серьезным проблемам в случае увольнения квалифицированных специалистов.

Рекомендация.

МФКР и ГУИС должен принять срочные меры по утверждению кадровой политики, которой будут четко описаны процедура приема на работу и увольнения сотрудников ГУИС, а также описаны роль и обязанности сотрудников в рамках организации, квалификационные требования и требования к обучению.

ГУИС должен согласовать с МФКР меру ответственность за оказание технической поддержки в РОКах и процедуру приема на работу региональных специалистов.

МФКР должен утвердить штатное расписание ГУИС, так как штатное расписание и бюджет являются неотъемлемой частью годового плана работы ГУИС.

Наблюдение 8.

Согласно пункту 5 главы 3 “Положения об Управлении информационных технологий и модернизации МФКР” ИТ управление “осуществляет мониторинг и анализ работы центрального аппарата Министерства, его территориальных органов и подведомственных подразделений по вопросам внедрения автоматизированных систем управления государственными финансами”.

Учитывая, что Управление ИТ при МФКР является одной из сторон, ответственной за контроль соблюдения регламентов, утвержденных Приказом Министерства об утверждении технической документации функционирования АИС и баз данных Министерства (№ 206-П от 13.12.2013), необходимо на регулярной основе повышать потенциал сотрудников управления ИТ и обучать основам информационной безопасности.

Риск.

Слабая система внутреннего контроля.

Рекомендация.

ИТ управление должно принять меры по выполнению целей и задач, указанных в “Положение об Управлении информационных технологий и модернизации МФКР” и по отношению к ГУИС. Рекомендуется усилить контрольные функции ИТ Управления.

5.2 Функционирование информационной системы.

5.2.1 Управление изменениями.

Основной целью данного вопроса является получение доказательств того, что электронная система поддержки Service Desk, введенная в действие Приказом МФКР №68-П от 05.04.2012 для регистрации заявок на изменения, поступающих от пользователей и контроля выполнения зарегистрированных запросов пользователей, отвечает требованиям пользователя.

Наблюдение 9.

В Service Desk недостаточно доработана система закрытия запросов, после их подтверждения. После выполнения запросов специалистами ГУИС многие запросы остаются не закрытыми, так как пользователи системы в лице сотрудников ЦК МФКР не подтверждают успешное выполнение запроса (закрыть запрос). Не проводится обучение сотрудников.

Риск.

Задержка в закрытии уже выполненных запросов может привести к задержке выполнения других запросов и повторному выполнению уже подтвержденных запросов.

Рекомендация.

ГУИС совместно с ИТ управлением должны провести обучение пользователей системы по работе системы Service Desk, в части процедур закрытия запросов. Довести до сведения каждого уже разработанную инструкцию для пользователя.

Наблюдение 10.

Пользователи системы (сотрудники ЦК МФКР и РОК) при оформлении запросов в Service Desk не имеют знаний о том, к какому из типов относится их запрос. В результате, наименование типа запроса не соответствует содержанию запроса, что влияет на сроки их рассмотрения со стороны ГУИС.

Риск.

Имеется риск того, что запросы с высоким уровнем приоритетности могут быть получены ГУИС как запрос с низким уровнем приоритетности и наоборот.

Рекомендация.

ГУИС совместно с ИТ управлением должны провести обучение для сотрудников ЦК МФКР и РОК по использованию и работе системы Service Desk, в части определения типа запросов.

Наблюдение 11.

В ходе аудита был направлен тестовый запроса о присвоении пароля новому сотруднику через Service Desk. Ответ был получен с нарушением двух установленных правил:

- В ответе на запрос было указано, чтобы пользователь использовал стандартный пароль, несмотря на то, что пароли уволившихся сотрудников должны быть аннулированы, а новым сотрудникам должны присваиваться новые пароли;
- Ответ был получен через 2 дня вместо 2 часов.

Также, были отмечены задержки в реагирования на другие запросы пользователей на срок более 5 месяцев (ЦКМФ).

Риск.

Существует риск остановки работы ИС.

Рекомендация.

ИТ Управлению МФКР должен осуществлять периодически мониторинг и контроль выполнения запросов пользователей на изменения через систему Service Desk .

Наблюдение 12.

Отсутствует журнал регистрации инцидентов. Во время аудита имел место случай остановки системы в Чон-Алайском РОК на 4 дня. Заявка о техническом сбое поступила сотруднику Управления ИТ по телефону, так как из-за отсутствия связи отключился Service Desk. Данный инцидент не был зарегистрирован ни в электронном виде, ни в виде записи в журнале инцидента.

Риск.

Риск остановки работы ИС на длительное время и несанкционированного доступа.

Рекомендация.

ИТ Управлению при МФКР должен создать механизм для регистрации, мониторинга и контроля всех инцидентов и проводить анализ рисков с целью предотвращения повторяющихся ошибок и сбоев системы. В целях обеспечения мониторинга инцидентов, управления системой Service Desk передать в управление ИТ.

5.3 Разработка и закупка.

5.3.1 Требования к разработке программного обеспечения ИС «IS:Казна.Бюджет».

Основной целью данного вопроса является получение доказательств того, что требования заказчика на разработку ИС четко описаны.

Наблюдение 13.

Требования к разработке программного обеспечения (техническое задание) информационной системы “IS Казна.Бюджет (далее ИС) отсутствуют, так как данная ИС является модернизированной версией программы “IS:Казна”, разработанной согласно инструкции о порядке ведения учета доходов государственного бюджета и доходов, поступивших от операций с активами и обязательствами, в системе ЦК МФКР.

В связи с этим, основные требования для разработки модулей ИС были указаны в следующих документах:

1. план мероприятий "Экономика и безопасность" на 2011 год по реализации программы Правительства Кыргызской Республики (пункт 62), где указаны следующие функции перехода на единый казначейский счет (ЕКС):
 - каждому региональному отделению казначейства (РОК) должны быть присвоены банковские идентификационные коды (БИК);
 - лицевые счета учреждений должны быть приведены в соответствие с требованиями НБКР (имеют 16 разрядов, контрольная цифра и т.д.);
 - должны быть разработаны модули по обработке SWIFT файлов для работы в системе пакетного клиринга (СПК) и grossовой системе расчетов (ГСРРВ);
 - в заявках на кассовый расход должны быть добавлены поля, необходимые для создания платежных поручений.
3. Инструкции, положения и другие НПА, регламентирующую работу ЦК МФКР.

Риск.

Отсутствие утвержденного технического задания с указанием всех требований не предоставляют заказчику возможности осуществлять мониторинг и контроль исполнения технического задания.

Рекомендация.

Для разработки ИС МФКР, являясь заказчиком, должен четко сформулировать и утвердить требования к ИС, которые затем будут утверждены в виде технического задания. В процессе формулирования требований к ИС должны участвовать пользователи системы, технический персонал, а также эксперты. Данное техническое задание является основой для принятия решения либо о разработке дополнительных модулей специалистами ГУИС, либо подписания прямого соглашения с разработчиками, либо закупке нового программного обеспечения.

5.4 Информационная безопасность.

5.4.1 Политика безопасности.

Основной целью данного вопроса было получение подтверждения безопасности организации внутренних и внешних коммуникаций и защиты от несанкционированного доступа, копирования или просмотра конфиденциальной информации.

Наблюдение 14.

В Иссык-Атинском РОК часть компьютеров не входят в домен и не подчиняются общим правилам безопасности. Также, для пользователей открыт административный доступ.

Риск.

Риск использования несанкционированного программного обеспечения.

Рекомендация.

ИТ Управлению МФ КР необходимо провести ревизию программного обеспечения в районных отделениях, с целью предотвращения использования несанкционированного программного обеспечения. Также необходимо провести аудит контроля доступа, с сопоставлением учетных записей и разрешенных прав в соответствии с их функциональными обязанностями. На всех компьютерах реализовать доменную систему, которая позволяет в значительной степени повысить безопасность сети, управляя разрешениями, политиками безопасности, и все ПК должны иметь общую базу данных, общую политику безопасности

Наблюдение 15.

Аудитом было выявлено много не лицензированных программных продуктов, в том числе игровых, установленных на персональных компьютерах сотрудников Иссык-Атинского РОК.

Риск.

Риск использования несанкционированного программного обеспечения. Нарушение законодательства КР об интеллектуальной собственности.

Рекомендация.

ИТ Управлению МФ КР должно принять меры по удалению программного обеспечения, не имеющего лицензии или не разрешенного руководством к использованию в районных отделениях. Также необходимо пересмотреть и обновить регламент пользователей РОК в политике информационной безопасности, где будет прописано права и обязанности пользователей РОК. Документированная ПИБ должна быть утверждена руководством опубликована и доведена до сведения всех сотрудников ЦА, ЦК, РФО и РОК МФКР. Политика информационной безопасности должна пересматриваться через запланированные интервалы времени, а также в случае влияющих на нее существенных изменений, чтобы обеспечить ее непрерывное соответствие реальному положению дел, достаточность и эффективность.

Наблюдение 16.

Установлены антивирусные базы, которые не обновлялись более чем один месяц.

Риск.

Существует риск потери информации в результате заражения “вирусом”.

Рекомендация.

ИТ Управление должно принять срочные меры по установлению на всех персональных компьютерах лицензионного антивируса с актуальными антивирусными базами, системой централизованного обновления и мониторинга для более быстрого реагирования на возникшие угрозы.

Наблюдение 17.

На компьютере заместителя начальника Свердловского РОК имеется доступ к интернету с другой линии, минуя корпоративную сеть, то есть имеется возможность выходить в интернет бесконтрольно.

Риск.

Риск несанкционированного доступа к информации.

Рекомендация.

ИТ управление должно принять меры по ограничению доступа к интернету с другой линии, минуя корпоративную сеть. Все персональные компьютеры региональных отделений должны иметь единую точку выхода в интернет (если это обусловлено регламентом), и весь трафик должен проходить через межсетевой экран и соответствующие фильтры. Пересмотреть и обновить регламент пользователей РОК в политике информационной безопасности, где будет прописаны права и обязанности пользователей РОК. Должен существовать официальное дисциплинарное наказание в отношении сотрудников, допускающих нарушение безопасности.

Наблюдение 18.

Отсутствует журнал проведения профилактических работ серверного оборудования и персональные компьютеры в РОК.

Риск.

Риск остановки работы ИС.

Рекомендация.

ИТ управление должен вести контроль проведения профилактических работ с регистрацией в журнале профилактических работ и указанием, даты проведения работ, вида оборудования, выявленных проблем и принятых мер. Заполненный журнал профилактических работ помогает более эффективно решать повторно возникающие проблемы и принимать превентивные меры. Должны быть установлен график проведения профилактических работ серверных оборудования в соответствии с согласованной политикой информационной безопасности. Действия системных администраторов должны контролироваться и фиксироваться соответствующими актами по проведению профилактических работ.

Наблюдение 19.

Отсутствует акт испытания пожарной системы.

Риск.

Риск потери имущества вследствие пожара.

Рекомендация.

ИТ управление и ГУИС должны не реже одного раза в год проводить испытания систем контроля пожаротушения. Пожарная система должна тестироваться через запланированные интервалы времени, чтобы обеспечить ее непрерывное соответствие требований пожарной безопасности, достаточность и эффективность, в соответствии с согласованной политикой пожарной безопасности. Процедуры испытания должны протоколироваться и фиксироваться соответствующими актами по проведению тестирования пожарной системы.

5.4.2 Конфиденциальность.

Основной целью данного вопроса было получение подтверждения того, что в МФКР исполняется Постановление Правительства Кыргызской Республики от 7 июля 1995 №267/9 “Об утверждении Перечня главнейших сведений, составляющих государственную тайну” в отношении ИС “IS-Казна. Бюджет”.

Наблюдение 20.

В ответ на запрос о предоставлении НПА, устанавливающего степень секретности сведений, содержащихся в работах и документах и внутриведомственного перечня ИС, подлежащих защите от несанкционированного доступа (исх №01-10/1555 от 10 ноября 2014), аудитом был получен ответ о том, МФКР руководствуется Постановлением Правительства Кыргызской Республики от 7 июля 1995 №267/9 “Об утверждении Перечня главнейших сведений, составляющих государственную тайну”.

Аудитом отмечено, что в нарушение Постановления ПКР, в МФКР отсутствует утвержденный ведомственный перечень сведений, подлежащих засекречиванию и не установлена степень секретности, относящаяся к его деятельности с учетом внутриведомственного перечня.

Риск.

Риск несанкционированного доступа к информации.

Рекомендация.

Во исполнение Постановления Правительства Кыргызской Республики от 7 июля 1995 №267/9 “Об утверждении Перечня главнейших сведений, составляющих государственную тайну”, МФ КР должен утвердить ведомственный перечень сведений, подлежащих засекречиванию и установить степень секретности, относящуюся к их деятельности с учетом внутриведомственного перечня.

Наблюдение 21.

Аудитом отмечено, что некоторые сотрудники ГУИС, имеющие по профессиональной необходимости постоянный доступ ко всем данным ИС, а также свободный доступ в ЦОД и РЦОД, не имеют доступа к секретным документам по форме №26. В частности, аудиту не был предоставлен документ, подтверждающий доступ к секретной информации Токочева Руслана - Директора ГУИС, назначенный Распоряжением Премьер Министра Кыргызской Республики от 26 июня 2014 года №287.

Риск.

Отсутствие официального доступа к информации по форме №26 ведет к риску несанкционированного доступа к информации.

Рекомендация.

Несмотря на то, что все требования по обеспечению конфиденциальности сотрудниками ГУИС описаны в должностных инструкциях специалистов информационных систем, ГУИС должен получить доступ к секретной информации по форме №26 для всех сотрудников, имеющих постоянный доступ ко всей информации ИС, а также свободный доступ в ЦОД и РЦОД.

5.4.3 Доступ в ЦОД и РЦОД.

Основной целью данного вопроса было предоставление оценки соблюдения условий доступа в ЦОД и РЦОД.

Наблюдение 22.

В ГУИС внедрена система защиты на базе аппаратно-программного комплекса CISCO, ASA 5510, 5520 со встроенным модулем IPD. Все основное оборудование на уровне ядра сети дублируется для обеспечения надежности работы и балансировки нагрузки. Все региональные подразделения соединены VPN туннелем с использованием IPsec.

Для обеспечения безопасности сети в ГУИС используется фаервол ASA 5510, 5520. Доступ к файловым серверам и программным продуктам имеют авторизированные пользователи.

Тем не менее, аудитом отмечен факт физического доступа к роутерам и коммутаторам не авторизованных специалистов.

Риск.

Риск несанкционированного доступа к оборудованию.

Рекомендация.

Все шкафы с серверным или сетевым оборудованием должны быть оборудованы замками. Доступ к оборудованию должен осуществляться только сотрудникам, имеющим допуск.

Наблюдение 23.

Серверный шкаф с активным оборудованием не закрыт на замок.

Риск.

Риск несанкционированного доступа к оборудованию. Возможность получения административных прав к коммутаторам и маршрутизаторам, в случае обнуления пароля на IOS.

Рекомендация.

МФ КР должен принять срочные меры к тому, чтобы телекоммуникационные и силовые кабели, сетевые шкафы, коммутаторы и роутеры передающие данные или

поддерживающие информационные сервисы были защищены от несанкционированного доступа и повреждения соответствующими механизмами контроля входа, в частности замком, обеспечивающим возможность доступа только для заведующих РОКов. Назначить ответственным за физический доступ к активным сетевым оборудованьям, к роутерам и коммутаторам заведующих РОК. Пересмотреть и обновить регламент пользователей РОК, где будут прописаны права и обязанности пользователей РОК. После осуществления технического обслуживания следует закрывать шкафы на замок.

Наблюдение 24.

Отмечены случаи, когда доступ к системе уволенных сотрудников не заблокирован.

Риск..

Риск несанкционированного доступа к информации.

Рекомендация.

МФКР должен утвердить список лиц, имеющих удаленный доступ к системе. Согласно политики безопасности, доступ к системе уволившихся сотрудников должен быть автоматически заблокирован. ГУИС согласовывать кадровую политику с МФКР.

Наблюдение 25.

Согласно “Регламента доступа в операторскую и серверные помещения ЦОД и РЦОД”, подписанного директором ЦК МФКР Темирбековым М. от 16.03.2011,. доступ в серверные помещения ЦОД и РЦОД должен осуществляться согласно списка, приложенного к Регламенту. Список сотрудников, имеющих доступ в ЦОД и РЦОД (Приложение к Регламенту), не обновлялся с 2011 года. В нарушении пункта 3.5 контроль актуальности списка не осуществлялся. В списке до сих пор указаны фамилии уволившихся сотрудников.

Риск.

Риск несанкционированного доступа к информации и оборудованию.

Рекомендация.

МФ КР должен сочно внести изменения в Регламент доступа в ЦОД и РЦОД. Осуществлять контроль актуальности списка на постоянной основе. Список сотрудников МФКР, ЦК МФКР и ГУИС, должен быть вывешен на видном месте ЦОД и РЦОД. Доступ лиц, не включенных в список доступа, должен осуществляться только по письменному разрешению ответственных сотрудников МФКР или ЦК МФКР, которые должны храниться в отдельной папке.

Наблюдение 26.

В журнале обнаружены следующие недостатки заполнения:

1. в колонке «Цель доступа» отсутствует детальное объяснение цели доступа зарегистрированных лиц.
2. нарушен порядок нумерации или нумерация отсутствует, что приводит к искажению информации о количестве лиц, посетивших серверное помещение.
3. практически везде отсутствуют подписи лиц, во многих случаях отсутствует «время входа» в серверное помещение и «время выхода» из серверного помещения.

4. в журнале имеется пустой лист (6 стр.). Регистрация посещений в Журнале заканчивается на 8 странице. Последние посещения, датированные декабрем 2014 года, зарегистрированы на 7 странице (можно предположить, что страница до регистрации оставалась пустой).
5. в журнале были зарегистрированы лица, посетившие ЦОД с целью ознакомления с сервером, не имеющие отношения ни к какой категории лиц, указанных в пункте 2.2 регламента доступа в ЦОД. Например: специалисты Министерства здравоохранения КР, ГП «Инфоком» при ГРС, представители АБР и т.д.
6. журнал ведется неаккуратно, имеется много исправлений в дате и времени посещений.
7. в Журнале нет разделения между посторонними лицами и сотрудниками ГУ ИС.

Риск.

Риск несанкционированного доступа в ЦОД и РЦОД.

Рекомендация.

Записи в журнале должны осуществляться аккуратно, без исправлений и данные о посетителях должны включать цель посещения, указанную в письменном разрешении, выданном МФКР или ЦК МФКР. ГУИС согласовывать кадровую политику с МФКР.

5.4.4. Инвентаризация.

Основной целью данного вопроса было получение доказательства о физическом наличии компьютерного, серверного и телекоммуникационного оборудования, переданного ГУИС согласно Договора МФ КР и ГУИС о передаче оборудования в безвозмездное временное пользование.

Наблюдение 27.

По результатам физической инвентаризации выявлена недостача двух ноутбуков на сумму 118754 сом: Ноутбук Pro Book HP4320s (инв. номер 01362085) и Ноутбук Pro Book HP4320s (инв. номер 01362084), которые, по словам специалиста ГУИС, находятся у ранее уволившихся сотрудников

Риск.

Риск хищения.

Рекомендация.

ГУИС должен восстановить два ноутбука или произвести возврат стоимости оборудования в сумме 118754 сом.:

Наблюдение 28.

Серийные номера оборудования, указанные в “Инвентарной карточке по использованию техники ЦОД от 12.06.2014” не соответствуют серийным номерам оборудования, указанных в “Перечне оборудования для передачи в безвозмездное пользование”.

Риск.

Риск возможного хищения оборудования.

Рекомендация.

МФКР и ГУИС должны привести в соответствие инвентарные и серийные номера серверов.

Наблюдение 29.

Серверные шкафы, установленные в РЦОД, не поставлены на баланс и не включены в инвентарную опись. В ЦОД и РЦОД, шкафы не пронумерованы и отсутствует перечень серверов на шкафах, что затрудняет поиск нужных серверов.

Рекомендация.

МФ КР должен принять срочные меры по постановке на балансовый учет серверных шкафов установленных в РЦОД.

Наблюдение 30.

В серверном помещении ЦОД обнаружены излишки оборудования на сумму около **932419** долларов США, установленного по контракту с компанией Free balance. **Акт приема передач между МФКР и Free Balance не подписан.** Данное оборудование не включено в инвентарную опись и не поставлено на баланс в МФ КР. Несмотря на то, что данное оборудование находится на территории, куда имеют доступ сотрудники ГУИС и третьи лица, Акт приема передачи или Договор на временное хранение между МФКР и ГУИС не были оформлены.

Аудитом получены следующие комментарии МФКР:

МФКР сообщает о том, что в настоящее время контракт с компанией Free Balance юридически еще не расторгнут. В этой связи, не исключаются затяжные судебные разбирательства. При этом, за оборудование, которое находится в ЦОД, МФКР **не произвело оплату по объективным причинам.** Согласно условиям контракта оплата осуществляется за установку информационной системы в целом, а не отдельно за оборудование.

Риск.

Риск хищения оборудования.

Рекомендация.

МФ КР должен регулярно проводить проверку на сохранность оборудования на сумму около 932419 долларов США, установленного по контракту с компанией Free balance, с оформлением письменного Акта и опечатывать серверные шкафы с оборудованием до решения данного вопроса. .

Наблюдение 31.

Вследствие отсутствия актов приема передач модулей ИС между ГУИС и МФКР, а также, в нарушение Приказа МФ КР от 24 мая 2014 №90-П “О мерах, связанных с принятием на баланс нематериального актива”, информационная система "IS Казна. Бюджет" не была поставлена на балансовый учет МФКР в виде нематериального актива, что является грубым нарушением “Закона о бухгалтерском учете КР”.

Рекомендация.

ГУИС должен в срочном порядке передать МФКР ключи и исходные коды от "IS Казна. Бюджет" с детальными описаниями и провести обучение. МФ КР должен принять срочные меры по постановке на балансовый учет нематериального актива ИС "IS Казна. Бюджет".

5.4.5 Политика резервного копирования ППО и СУБД «IS:Казна.Бюджет».

Основной целью данного вопроса было получение доказательства того, что политики резервного копирования соблюдаются.

Наблюдение 32.

Согласно Политики резервного копирования ППО и СУБД «IS:Казна.Бюджет», утвержденной директором ЦК МФКР в 2011 году, правила организации резервного копирования в ЦОД и РЦОД выглядят следующим образом:

1. Каждые 09:10, 12:30, 18:10 с понедельника по пятницу сервер база СУБД данных msc01-app01 резервирует на сервер резервного копирования msc01-bak01 в папку \\msc01-file01\nix_backup\budget\db\inc.
2. Каждые 30 минут с 9:00 до 22:00 с понедельника по пятницу сервер база данных bcc01-app01 резервирует на сервер резервного копирования bcc01-bak01 в папку\\msc01-file01\nix_backup\budget\db\inc.
3. Каждый день в 1:30 часа ночи сервер база данных msc01-app01 резервирует на сервер резервного копирования msc01-bak01 в папку\\msc01-file01\nix_backup\budget\db\full
4. Ежедневно в 1:30 часа ночи сервер база данных bcc01-app01 резервирует на сервер резервного копирования bcc01-bak01 в папку\\bcc01-file01\nix_backup\budget\db\full

Ежедневно копия резервных системы дублируется на ленточное устройство, расположенных в ЦОД и РЦОД соответственно.

В настоящее время резервное копирование ИС осуществляется только один раз в день, в 1:30 часа утра. Остальные пункты организации резервного копирования не выполняются.

Риск.

Риск потери информации за предыдущий период.

Рекомендация.

МФКР должен обновить Политику резервного копирования ППО и СУБД «IS:Казна.Бюджет», утвержденной директором ЦК МФКР в 2011 году.

Наблюдение 33.

Отсутствует контроль и мониторинг выполнения Политики резервного копирования со стороны ИТ управления МФКР.

Рекомендация.

ИТ управление должно осуществлять контроль результатов всех процедур резервного копирования не реже одного раза в неделю.

5.5 Контроль приложений.

Наблюдение 34

В Свердловском и Иссык-Атинском РОКах были возбуждены уголовные дела, связанные с искажениями отчетности РОК путем внесения изменений в коды платежей, что привело к хищениям государственных средств.

После проведения служебной проверки, ЦК МФ направил поручение в ГУИС о необходимости закрытия доступа сотрудникам РОК в программное обеспечение в части выгрузки и обработки банковской выписки, в целях исключения человеческого фактора при внесении изменений в выписку банка. ГУИС разработал отчет, который позволяет сотрудникам ЦК МФКР сравнивать коды платежей, вводимые специалистами РОК с кодами платежей, указанными в данных Банка-агента. В ходе проверки, главным специалистом Отдела анализа и методологии ЦК МФ Усубакуновым Ж. выборочным способом распечатаны выписки РОК за январь 2013 г., в котором прослеживается

внесение изменений сотрудниками РОК в коды платежей и за август 2013 г. (после внесения изменения в программное обеспечение ГУИС), в котором данные кодов платежей, вводимые сотрудниками РОК, идентичны данным Банка-агента.

Тем не менее, в Иссык-Атинском РОК аудитом был обнаружен отчет, где сотрудник РОК имеет возможность изменить лицевой счет.

Риск.

Риск недостоверности отчетных данных.

Рекомендация.

ЦК МФКР и ГУИС должны предпринять меры по исключению возможности пользователям вносить изменения в лицевые счета налогоплательщика.

Наблюдение 35

При встречном аудите РОК Свердловского района установлено, что общая сумма, поступившая за 2014 год по следующим неналоговым платежам: «Государственная пошлина», «Плата за выдачу сертификатов и других разрешительных документов», «Плата за выдачу лицензий», составила **38,9 млн. сом**. Данная сумма, согласно раздела 8 Закона КР «О неналоговых платежах», была зачислена на счет Управления Государственной налоговой службы по Свердловскому району г. Бишкек. В ответ на запрос аудита, был получен ответ от ГНС Кыргызской Республики о том, что ГНС КР **не подписывает актов сверки** так как не является администратором данных счетов, несмотря на то, что, согласно Закону, “контроль за правильностью и своевременностью уплаты неналоговых платежей в бюджет осуществляют налоговые органы”.

Аудитом получены следующие комментарии МФКР:

для обеспечения прозрачности исполнения бюджета, учета поступления доходов в разрезе министерств и ведомств, предотвращения возможных хищений бюджетных средств был разработан проект Постановления ПКР «Об администраторах поступлений в республиканский и местные бюджеты Кыргызской Республики». Проектом предлагается утвердить Перечень главных администраторов ресурсов, определить их полномочия и обязанности по администрированию неналоговых доходов, в соответствии с установленными законодательными актами.

Риск.

Отсутствие контроля за правильностью и своевременностью уплаты неналоговых платежей в бюджет (РОК) ведет к хищениям государственных средств.

Рекомендация.

МФКР и ЦК МФКР должны определить все виды неналоговых платежей по которым ГНС не осуществляют акты сверок с РОК. Определить администраторов данных платежей и в дальнейшем осуществлять акты сверок по поступлениям.

Перечень регламентов и положений

МФ КР				
№	Название	№	Дата	Подписан
1	Договор о передаче оборудования в безвозмездное временное пользование между МФ КР и ГУИС	25	5/3/2011	Статс-секретарь МФ КР Шайдиева Д.Дж.; Директор ГУИС Шаикова А.К.
2	Положение порядке функционирования АИС и баз данных МФ КР	б/н	12/18/2013	Утверждено Приказом Министра финансов №206-П от 18.12.2013
3	Приказ об информационном портале ГОСУДАРСТВЕННЫЕ ИНФОРМАЦИОННЫЕ РЕСУРСЫ КР	114-П	6/18/2012	Министр финансов Жапаров А.У.
4	Приказ об утверждении паспорта проекта и плана работ по разработке портала и внешней помощи	166-П	8/24/2012	Министр финансов Жапаров А.У.
5	Приказ об утверждении технической документации функционирования автоматизированных информационных систем и баз данных МФ КР	206-П	12/18/2013	Министр финансов Лаврова О.В.
6	Приказ об утверждении электронной системы поддержки пользователей ServiceDeskНаумен	68-П	4/5/2012	И.О. министра финансов Темирбеков М.
7	Регламент информационной безопасности при использовании интернет-ресурсов в МФ КР	б/н	12/18/2013	Утверждено Приказом Министра финансов №206-П от 18.12.2013
8	Регламент информационной безопасности при использовании корпоративной эл. почты в МФ КР	б/н	12/18/2013	Утверждено Приказом Министра финансов №206-П от 18.12.2013
9	Регламент сопровождения автоматизированной информационной системы казначейства IS Казна.Бюджет	б/н	12/18/2013	Утверждено Приказом Министра финансов №206-П от 18.12.2013

10	Регламент по управлению доступом, подключению и технич.поддержки пользователей информац.сист.казн-ва IS Казна.Бюджет	б/н	12/18/2013	Утверждено Приказом Министра финансов №206-П от 18.12.2013
----	--	-----	------------	--

ЦК МФ КР				
№	Название	№	Дата	Подписан
1	Положение о порядке внесения изменений в программное обеспечение IS.Казна.Бюджет	б/н	9/20/2011	Директор ЦК Темирбеков М.; Согласовано: Директор ГУИС Шаикова А.К.
2	Регламент доступа в операторскую и серверные помещения ЦОД и РЦОД МФ КР	б/н	10/3/2011	Директор ЦК Темирбеков М.; Согласовано: Директор ГУИС Шаикова А.К.
3	Соглашение о безвозмездном оказании услуг	1	12/30/2011	Директор ЦК Темирбеков М. и Директор ГУИС Шаикова А.К.

ГУИС МФ КР				
№	Название	№	Дата	Подписан
1	Приказ о принятии во временное пользование оборудования ЦОД и РЦОД	7-пн	7/7/2011	Директор ГУИС Шаикова А.К.
2	Регламент техобслуж и ремонта комп оборудования ГУИС	04-07-2013 2013-09-26 СТ.БП.3.2-2013	7/29/2013	Утверждено Приказом Директора ГУИС №21-1-4/11 от 29.07.2013
3	Стандарт ГУИС техподдержки ИС	СТ.БП.3.2-2013	7/29/2013	Утверждено Приказом Директора ГУИС №21-1-4/11 от 29.07.2013
4	Стандарт ГУИС Управление информационной безопасностью	СТ.УП.3-2013	7/29/2013	Утверждено Приказом Директора ГУИС №21-1-4/11 от 29.07.2013
5	ДИ администратора инженерных систем	б/н	10/22/2012	Утверждено Приказом Директора ГУИС №14-пн от 22.10.2012
6	ДИ Администратора серверов отдела информационных систем	б/н	10/22/2012	Утверждено Приказом Директора ГУИС №14-пн от 22.10.2012

7	ДИ Администратора сервисов отдела информационных систем	б/н	10/22/2012	Утверждено Приказом Директора ГУИС №14-пн от 22.10.2012
8	ДИ Администратора систем отдела информационных систем	б/н	10/22/2012	Утверждено Приказом Директора ГУИС №14-пн от 22.10.2012
9	ДИ Заместителя начальника отдела информационных систем	б/н	10/22/2012	Утверждено Приказом Директора ГУИС №14-пн от 22.10.2012
10	ДИ Начальника отдела информационных систем	б/н	10/22/2012	Утверждено Приказом Директора ГУИС №14-пн от 22.10.2012
11	ДИ аналитика отдела управления проектами	б/н	10/22/2012	Утверждено Приказом Директора ГУИС №14-пн от 22.10.2012
12	ДИ заместителя начальника отдела управления проектами	б/н	10/22/2012	Утверждено Приказом Директора ГУИС №14-пн от 22.10.2012
13	ДИ начальника отдела управления проектами	б/н	10/22/2012	Утверждено Приказом Директора ГУИС №14-пн от 22.10.2012

Приложение 2.

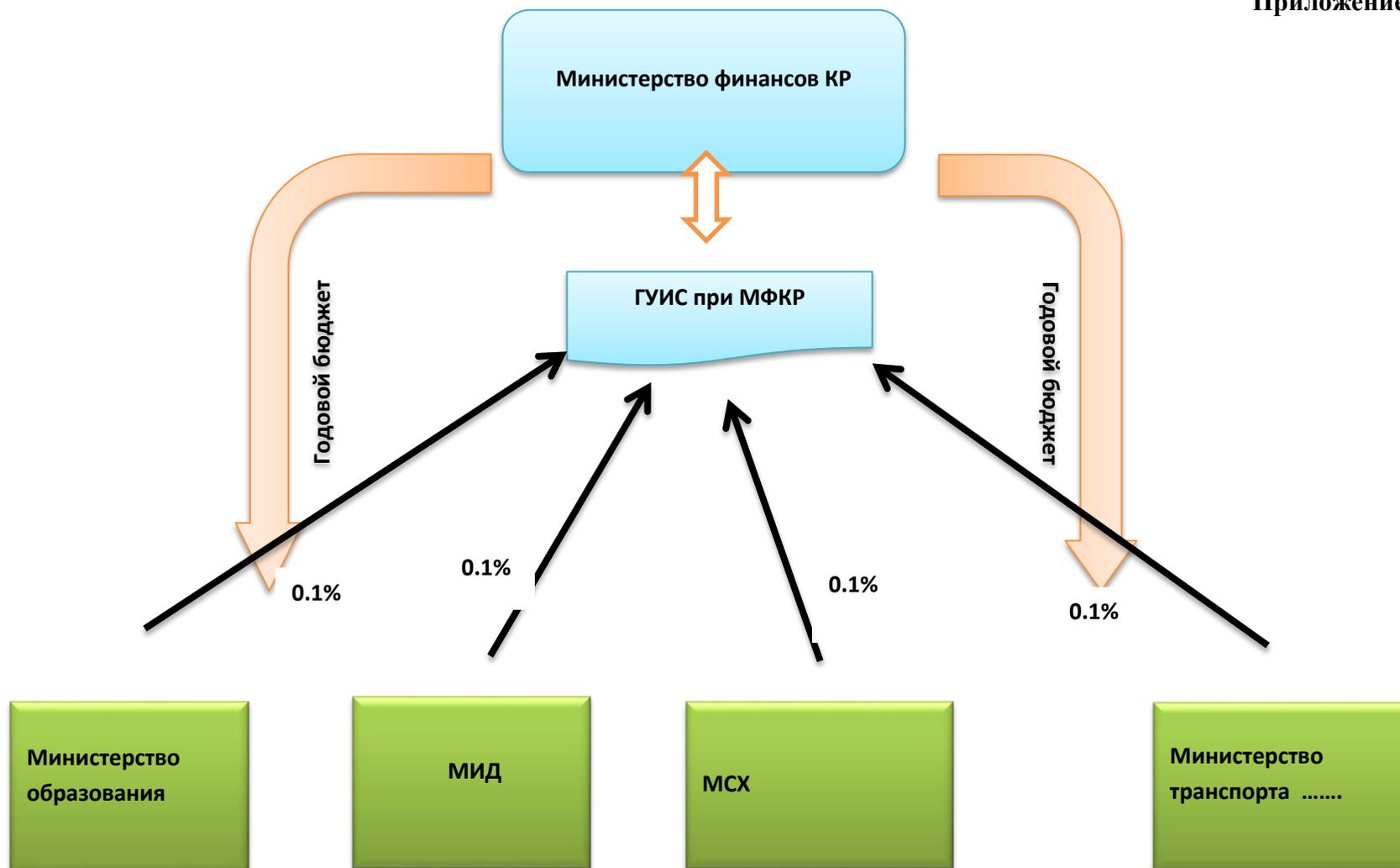
За период с 2009 по 2012 специалистами ГУИС были разработаны следующие программные продукты:

№	Название продукта	Статус	Заказчик
1	IS:Kazna. Budget [2011-3] http://budget.infosystema.kg	Завершен	МФКР
2	IS: Kazna. Report -2011-1 http://report.infosystema.kg	Завершен	МФКР
3	IS:Contract -2011-1 http://budget.infosystema.kg	Завершен	МФКР
4	IS:Personnel- 2010-1 https://212.112.104.44	Завершен	ГКС
5	IS:Test. 2010-1	Завершен	ГКС
6	e-Portal “Open Budget” [2012-1] http://budget.okmot.kg	Завершен	МФКР
7	e-Portal “Economic map”[2012-1] http://map.okmot.kg	Завершен	МФКР
8	e-Portal “Government e-Procurement”. 2012-1 http://oldzakupki.okmot.kg	Завершен	МФКР
9	e-Portal “Government e-Procurement”. 2012-2 http://zakupki.okmot.kg	Завершен	МФКР
10	Web application “Card ”	Завершен	МФКР
11	Web application “Card - Questionnaire”. 2013-1 http://budget.infosystema.kg/kazna-card/	Завершен	МФКР
12	АИС:РАГС (ЗАГС). 2012-1 http://zags.okmot.kg	Завершен	ГРС
13	АИС:СЭД. 2012-1 http://sed.okmot.kg	Завершен	Аппарат Правительства КР
14	Official web-site of Learning Center under the MoF KR [2012-1] http://training.okmot.kg	Завершен	Учебный центр при МФКР
15	e-Portal “External Support”. 2012-1 http://donors.okmot.kg	Завершен	МФКР
16	Web application “ЕКС”. 2012-1	Завершен	МФКР
17	Official site of the Moscow district administration Chui oblast	Завершен	МРГА Чуйской области
18	State information ressources .2012-1 http://www.okmot.kg	Завершен	МФКР
19	E-mail Service. 2012-1 http://mail.okmot.kg	Завершен	ГУИС
20	Unified Register of public services [2012-1]	Завершен	ГУИС

	http://services.okmot.kg		
21	e-Catalogue of state agencies. 2012-1	Завершен	ГУИС
	http://address.okmot.kg		
22	АИС:«Medical Certificate»	Завершен	Министерство здравохранения
	med.okmot.kg		
23	e-Portal for electronic appeals of citizens to state agencies of Kyrgyz Republic	Завершен	Аппарат Правительства КР
	http://kattar.kg		
24	Fuel map	Завершен	Аппарат Правительства КР
	http://ozp.okmot.kg		

Текущая схема финансирования ГУИС

Приложение 3



*0,1 % от годовой уточненной суммы сметы расходов по бюджетным средствам на отчетный финансовый год